DECRETO Nº 38.116 de 16 de janeiro de 2024

Institui a Política Municipal de Segurança da Informação do Município de Salvador na forma que indica.

O PREFEITO DO MUNICÍPIO DO SALVADOR, CAPITAL DO ESTADO DA BAHIA, no uso das atribuições, na forma do art. 52, V, da Lei Orgânica do Município e considerando a aprovação ad Referendum pelo Comitê Gestor de Segurança da Informação - CGSI, instituído pelo Decreto Municipal nº 36.565 de 24 de janeiro de 2023,

DECRETA:

Art. 1º Fica instituída a Política Municipal de Segurança da Informação do Município de Salvador com o objetivo de orientar todos os seus usuários para assegurar a efetividade da direção de gestão e suporte à segurança da informação de acordo com os requisitos legais, estatutários, regulatórios e contratuais na PMS, na forma dos seguintes documentos:

I - Política de Segurança da Informação - Anexo I;
II - Normas de Segurança da Informação - Anexo II;
III - Plano Tático de Segurança da Informação - Anexo III;
IV - Política de Backup e de Restauração de Arquivos Digitais da PMS - Anexo IV;
V - Plano de Continuidade de Negócios de TI - Anexo V;
VI - Plano de Gerenciamento de Vulnerabilidade - Anexo VI;
VII - Plano de Resposta a Incidente de Segurança - Anexo VII.

Art. 2º A Política Municipal de Segurança da Informação encontra-se amparada nos seguintes princípios:

I - Confidencialidade: propriedade da informação que só a torna disponível a indivíduos e entidades autorizadas;

II - Integridade: propriedade que garante que os dados sejam corretos, autênticos e confiáveis tal como foram fornecidos;

III - Disponibilidade: propriedade que garante a acessibilidade dos dados e sistemas quando necessário.

Art. 3º A Política Municipal de Segurança da Informação instituída por este Decreto deverá ser observada por todos os Órgãos e Entidades da Prefeitura Municipal de Salvador, que deverão promover, em articulação com a Secretaria Municipal de Inovação e Tecnologia - SEMIT, a adequação de suas estruturas à respectiva política em um prazo de até 06 (seis) meses.

Art. 4º Este Decreto entra em vigor na data de sua publicação.

GABINETE DO PREFEITO DO MUNICÍPIO DO SALVADOR, em 16 de janeiro de 2024.

BRUNO SOARES REIS
Prefeito

CARLOS FELIPE VAZQUEZ DE SOUZA LEÃO
Secretário de Governo

RODRIGO SANTOS ALVES
Secretário Municipal de Gestão

GIOVANNA GUIOTTI TESTA VICTER
Secretária Municipal da Fazenda

LUIZ CARLOS DE SOUZA
Secretário Municipal de Infraestrutura e Obras Públicas

ALEXANDRE ALMEIDA TINÔCO
Secretário Municipal de Ordem Pública

THIAGO MARTINS DANTAS
Secretário Municipal da Educação

LAZARO FRANÇA JEZLER FILHO
Secretário Municipal de Manutenção da Cidade

ANA PAULA ANDRADE MATOS MOREIRA
Secretária Municipal da Saúde em exercício

PEDRO CONDE TOURINHO
Secretário Municipal de Cultura e Turismo

JOÃO XAVIER NUNES FILHO
Secretário Municipal de Desenvolvimento Urbano

FABRIZZIO MULLER MARTINEZ
Secretário Municipal de Mobilidade

ANTONIO JOSÉ DA CRUZ JUNIOR MAGALHÃES
Secretário Municipal de Promoção Social, Combate à Pobreza, Esportes e Lazer

MARCELLE CARVALHO DE MORAES
Secretária Municipal de Sustentabilidade, Resiliência e Bem-Estar e Proteção Animal

IVETE ALVES DO SACRAMENTO
Secretária Municipal da Reparação

RENATA GENDIROBA VIDAL
Secretária Municipal de Comunicação

FERNANDA SILVA LORDELO
Secretária Municipal de Políticas para as Mulheres, Infância e Juventude

MILA CORREIA GONÇALVES PAES SCARTON
Secretária Municipal de Desenvolvimento Econômico, Emprego e Renda

SAMUEL PEREIRA ARAÚJO
Secretário Municipal de Inovação e Tecnologia

EDUARDO DE CARVALHO VAZ PORTO
Procurador Geral do Município

MARIA RITA GÓES GARRIDO
Controladora Geral do Município

ANEXO I

SALVADOR
PREFEITURA

Política de Segurança da Informação

Documento de Normas Administrativas

GSI – COGEL
V 2.0

DIÁRIO OFICIAL DO MUNICÍPIO

Histórico de revisões

Versão	Data	Alteração
Versão 1.0	19/01/2023	Lançamento da Primeira versão Adequada a política, termos tecnológicos, comunicadores instantâneos, suporte usuários via VPN e LGPD.
Versão	**Data**	**Alteração**
Versão 1.1	27/05/2023	Adequada a política, termos tecnológicos, comunicadores.
Versão	**Data**	**Alteração**
Versão 2.0	19/10/2023	Reestruturação de acordo com a Norma 27002:2022 e acolhimento de contribuições do Comitê de Segurança

Sumário

1 Contextualização....4
2 Glossário de Termos e Definições Utilizados Neste Documento....4
3 Sobre a Política de Segurança da Informação da PMS (PSI PMS)....5
4 Objetivos da Política de Segurança da Informação....5
5 Destinatários....5
6 Aplicabilidade da Política de Segurança da Informação....5
7 Princípios....6
8 Hospedagem de Servidores na COGEL....6
9 Contratação de terceiros....7
10 Desenvolvimento e Aquisição de Sistemas de Informação....7
11 Monitoramento e Controle....8
12 Proteção de Dados Pessoais....8
13 Responsabilidades Específicas....9
13.1 Dos Usuários em Geral....9
13.2 Dos Núcleos de TI da PMS....9
13.3 Dos Proprietários dos Ativos de Informação....10
13.4 Da Diretoria Técnica da COGEL – (COGEL/DITEC)....10
13.5 Da Gerência Especial de Segurança da COGEL (COGEL/GES)....11
13.6 Do Comitê Consultivo de Segurança (CCS)....11
13.7 Da Assessoria Jurídica da PMS....11
13.8 Da Gerência/Coordenação de Recursos Humanos....12
14 Divulgação da PSI e Documentos Correlatos....12
15 Disposições Gerais....12

1 Contextualização

A Prefeitura Municipal de Salvador (PMS) possui o compromisso de resguardar os serviços prestados à população de Salvador e proteger os dados dos cidadãos que estão sob sua guarda.

Neste sentido, a presente Política de Segurança da Informação da PMS (PSI PMS) apresenta diretrizes gerais de conduta, bem como obrigações a serem seguidas na PMS para mitigar eventuais riscos e danos relacionados a ameaças externas ou internas que possam impactar na confidencialidade, integridade e disponibilidade das informações sob sua guarda, objetivando garantir sua preservação.

Amparada nos preceitos da norma ISO 27001, em conformidade com a legislação vigente no Brasil e com base nas recomendações da ABNT NBR ISO / IEC 27002:2022, que orientam normas e procedimentos para a Gestão da Segurança da Informação (GSI), a PSI PMS define regras e responsabilidades gerais para a Segurança da Informação que devem ser observados por todos os órgãos e entidades que integram a PMS.

A fim de tratar de assuntos específicos, os seguintes documentos são complementares a esta PSI:

I. Normas de Segurança da Informação (NSI PMS);
II. Plano Tático de Segurança da Informação (PTS PMS);
III. Plano de Resposta a Incidentes (PRI PMS);
IV. Plano de Gerenciamento de Vulnerabilidades (PGV PMS);
V. Plano de Continuidade de Negócios (PCN PMS), contendo os seguintes subplanos:
    a. Plano de Gestão de Riscos e de Análise de Impacto (PGRAI);
    b. Plano de Contingência de TI (PCTI);
    c. Plano de Continuidade Operacional (PCO);
    d. Plano de Administração de Crises (PAC);
    e. Plano de Recuperação de Desastres (PRD);
VI. Política de Backup e de Restauração de Arquivos Digitais (PBR PMS).

2 Glossário de Termos e Definições Utilizados Neste Documento

Ativo: todo e qualquer bem da PMS que possui valor econômico, incluindo a informação, e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento.

Colaborador Interno: qualquer pessoa que execute atividade profissional e que possua algum tipo de vínculo profissional com a PMS (Exemplos: servidores públicos, funcionários, estagiários e prestadores de serviços).

Colaborador Externo: qualquer pessoa contratada por empresa terceirizada que execute alguma atividade profissional nas dependências da PMS, sem vínculo empregatício (Exemplos: consultores e prestadores de serviços).

Confidencialidade: garantia de que o acesso à informação seja realizado somente por pessoas que possuem autorizações para tal.

Comunicadores Instantâneos: aplicativos que permitem a interatividade entre pessoas através de troca de conversas e conteúdo em tempo real. Ex. WhatsApp, Telegrama, outros.

Dados Pessoais: informação relacionada a alguma pessoa natural identificada ou que possa ser identificável.

Dados Pessoais Sensíveis: dado pessoal sobre origem racial, ou étnica, convicção religiosa, opinião política, filiação à sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Disponibilidade: garantia de que os usuários obtenham acesso à informação e aos ativos informacionais quando necessário.

Informação: todo e qualquer conteúdo que possua valor. Pode estar armazenada para uso restrito ou exposta ao público para consulta.

Informação Sensível: toda informação sigilosa que, se divulgada, pode resultar em danos e/ou, prejuízos de qualquer ordem, perda de vantagem, inclusive financeira, bem como impacto negativo para a PMS.

Integridade: capacidade de garantir que a originalidade da informação, a fim de protegê-la contra alterações indevidas.

ISO 27002:2022: código de boas práticas com um conjunto completo de controles que fornece uma combinação genérica de controles de segurança da informação organizacional, de pessoas, física e tecnológica derivados das melhores práticas reconhecidas internacionalmente.

Parceiros: Empresas, órgãos públicos e demais instituições que possuem contrato com a PMS com objetivos em comum, unindo esforços em suas competências e expertises, sem que haja remuneração, mas apenas empenho de serviços por cada parte.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.

Usuário: todo funcionário, prestador de serviço, estagiário e afins que tenham acesso aos recursos tecnológicos oferecidos pela PMS.

3 Sobre a Política de Segurança da Informação da PMS (PSI PMS)

A Política de Segurança da informação (PSI) orienta e estabelece as diretrizes da Prefeitura Municipal de Salvador (PMS) para a proteção dos ativos de informação e da responsabilidade legal de todos os usuários. Consequentemente, deve ser respeitado e aplicado em todas as áreas da PMS.

Ela estabelece o compromisso da PMS em resguardar e proteger as informações que estão sob sua guarda, além de definir a governança de segurança da informação.

Essa PSI PMS exige o cumprimento de todas as leis e regulamentações aplicáveis e em vigor no Brasil, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD).

4 Objetivos da Política de Segurança da Informação

O objetivo da Política de Segurança da Informação (PSI) é o de orientar todos os seus usuários para assegurar a efetividade da direção de gestão e suporte à segurança da informação de acordo com os requisitos legais, estatutários, regulatórios e contratuais na PMS, através das seguintes ações:

- Documentar, organizar e sistematizar as decisões tomadas no planejamento da segurança;
- Unificar, formalizar e explicitar os objetivos da segurança;
- Servir como referência para as atividades e operações da segurança;
- Padronizar e orientar a prática da segurança na organização;
- Definir e orientar o emprego dos recursos disponíveis;
- Comunicar e divulgar responsabilidades, atividades e prazos;
- Orientar a como lidar com imprevistos;
- Auxiliar nas previsões orçamentarias.
-

5 Destinatários

A presente PSI PMS se destina a todos os seus colaboradores, estagiários, convidados, parceiros comerciais, fornecedores e prestadores de serviços que no âmbito da relação com a PMS possam acessar áreas, equipamentos, informações, arquivos, redes e dados de titularidade ou de terceiros sob a guarda da PMS, que para efeito de simplificação, passam a ser denominados “usuários” neste documento.

A PSI PMS é abrangente a todos os usuários independentemente do nível hierárquico ou função exercida na PMS.

6 Aplicabilidade da Política de Segurança da Informação

Os ativos de informação devem ser utilizados unicamente para a realização das atividades profissionais, com responsabilidade, com ética, e em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

A PSI PMS e as suas diretrizes serão revistos e atualizados anualmente ou sempre que surgirem fatos relevantes.
A PSI PMS abrange o gerenciamento das suas capacidades operacionais para a manutenção dos ativos de informação e continuidade dos negócios da PMS, cujas normas específicas são complementares e integram esta PSI PMS. Estas normas abrangem questões como o uso de e-mail, redes corporativas, Internet, uso de dispositivos móveis e comunicadores instantâneos.
Os usuários devem ser informados deste documento e de suas atualizações e observarem as diretrizes nele estabelecidas. Elas devem estar disponíveis em documento interno de fácil e sem restrições de acesso. Todos os usuários devem dar ciência da PSI PMS vigente em documento específico.
Em caso de dúvidas, os usuários devem buscar orientação no Setor ou Núcleo de Tecnologia da Informação (NTI).

7 Princípios

O compromisso da PMS com o tratamento adequado das informações se baseia nos seguintes princípios:

- Confidencialidade: propriedade da informação pela que não estará disponível ou divulgada a indivíduos, entidades ou processos sem autorização;
- Integridade: propriedade que garante que os dados sejam corretos, autênticos e confiáveis tal como foram fornecidos;
- Disponibilidade: propriedade que demonstra a acessibilidade que se tem dos dados e sistemas da empresa quando necessário pelos usuários.

8 Hospedagem de Servidores na COGEL

Com o objetivo de oferecer segurança, confiabilidade e disponibilidade, o Datacenter da COGEL oferece hospedagem na modalidade de "*colocation"* ou "hospedagem virtual de servidores", para atender as necessidades dos órgãos vinculados a PMS, uma vez que oferece recursos de segurança e possui equipe especializada e dedicada na manutenção e monitoramento dos serviços.
O datacenter da COGEL conta com uma estrutura planejada para atender as necessidades técnicas, com alto padrão de segurança. A infraestrutura atual tem as seguintes características:

- Espaço Físico: dispõe de espaço físico, como racks, gabinetes ou suítes, no qual os clientes podem instalar seus próprios servidores e equipamentos, além de um virtual center para alocação de máquinas virtuais, com tecnologia escalonável;
- Alimentação e Energia**:** a rede elétrica é estabilizada e redundante, possuindo gerador e nobreaks como backup do sistema elétrico, além de sistemas de backup de dados, para garantir a continuidade das operações;
- Controle Térmico**:** possui controle de temperatura e umidade, mantendo os equipamentos em funcionamento dentro das faixas de temperatura ideais;
- Conectividade de Rede: oferece conexões de rede confiáveis e de alta velocidade com links redundantes, para garantir a conectividade dos servidores, sites, sistemas e serviços;
- Segurança Física: oferece segurança física robusta, incluindo sistemas de controle de acesso, vigilância por vídeo, detecção de intrusos e a presença de GMS;
- Segurança Lógica: A COGEL conta com estrutura de segurança que visam a integridade, continuidade e confiabilidade do serviço hospedado;
- Monitoramento e Gerenciamento**:** conta com monitoramento integral (24/7) dos sistemas de energia, resfriamento e sistemas de segurança, bem como serviços de gerenciamento dos servidores e seus serviços, visando preservar a continuidade dos mesmos;
- Suporte Técnico**:** dispõe de equipe de suporte técnico especializada e dedicada, disponível para auxiliar os clientes com problemas de conectividade, segurança, hardware e software e qualquer outro aspecto relacionado à infraestrutura de TI;
- Ferramentas de Segurança: possui um arsenal de ferramentas que visam, garantir a continuidade, confiabilidade e segurança, contra ameaças internas e externas, com resposta a incidentes rápida;
- Resiliência e Redundância: O datacenter da COGEL conta com uma estrutura planejada que garante a redundância energética, rede e dados, garantindo um tempo de resposta a incidentes rápida para garantir o reestabelecimento do ambiente de forma segura e ágil;
- Resposta a Incidentes: A equipe técnica da COGEL realiza monitoramento e manutenção contínua do ambiente. Ela analisa os dados coletados e gera relatórios para uma resposta rápida a qualquer incidente que possa ocorrer na rede da PMS;
- Conformidade Legal e Regulamentar: As máquinas a serem hospedadas no regime de *colocation* ou hospedagem virtual no datacenter da COGEL, somente serão ingressadas após análise dos requisitos necessários.

O órgão da PMS interessado em alocar o seu servidor no Datacenter da COGEL, deverá abrir um chamado técnico para a COGEL/DITEC, solicitando a alocação do servidor de sua responsabilidade, informando as características técnicas e as necessidades a serem atendidas pela alocação, como rede elétrica, segurança e conectividade. A equipe do datacenter enviará para o solicitante um documento informativo sobre as políticas de uso do ambiente, para que este esteja em conformidade com as regras e boas práticas de utilização do serviço.
Se o órgão não possuir equipamento, este poderá solicitar hospedagem de seu sistema no datacenter da COGEL em um servidor dedicado ou máquina virtual, desde que informe as características necessárias para o funcionamento do ambiente como por exemplo, capacidade de processamento, memória necessária, armazenamento, conectividade, sistema operacional, serviços administrativos e de segurança.
Sistemas incompatíveis com o modelo de negócio da PMS não poderão ser alocados no datacenter da COGEL.
Inspeções de segurança devem ser autorizadas pelo solicitante do serviço para que a equipe do datacenter possa aferir a integridade, confiabilidade e e continuidade dos serviços.
As máquinas poderão ser alocadas no datacenter da COGEL somente após inspecionadas e em acordo com a PSI PMS.
Após as verificações técnicas, o solicitante da alocação assinará conjuntamente com o gerente responsável pelo datacenter da COGEL, um contrato de prestação de serviços no qual são explicitados os direitos e deveres de ambas as partes. Todas as informações referentes a prazos, suporte, valores, manutenção e inspeção de segurança serão descritos neste contrato.

9 Contratação de terceiros

Os administradores dos contratos da PMS devem notificar a Gerência Especial de Segurança (GES) através da Diretoria Técnica da COGEL (COGEL/DITEC), sempre que uma parceria ou vínculo empregatício com uma empresa terceirizada envolver acesso a informações e/ou recursos de TI. As responsabilidades de segurança da informação devem ser atribuídas na fase de contratação para que sejam incorporadas e monitoradas durante toda a vigência do contrato. Todos os contratos devem incluir um anexo ou cláusula de confidencialidade no uso das informações em conformidade com a LGPD vigente.
Em caso do não cumprimento da PGI por motivo de força maior, o responsável deverá formalizar e dar ciência à GES anteriormente à sua utilização.

10 Desenvolvimento e Aquisição de Sistemas de Informação

Os requisitos de segurança da informação, os aspectos legais envolvidos e planos de contingência devem ser identificados na fase de levantamento do projeto, os quais devem ser justificados, acordados e documentados. Estes requisitos devem ser verificados, testados e implementados na fase de execução do projeto.

Os sistemas, serviços ou produtos desenvolvidos que envolvam tratamento de dados pessoais deverão aplicar a regulamentação de privacidade adotada pela PMS desde a sua concepção.
O ambiente de produção e o ambiente de desenvolvimento técnico devem ser separados e rigorosamente controlados.

11 Monitoramento e Controle

O ambiente da organização, recursos de Tecnologia da Informação (TI), telefones, sistemas, computadores, dispositivos móveis e redes estão sujeitos a monitoração e registros em conformidade com a legislação vigente.
Devem ser criados e implementados controles apropriados para gerar registros de atividades em todos os pontos que a PMS julgue necessário para reduzir os riscos à segurança da informação. Assuntos técnicos e confidenciais que requerem acesso por equipes ou indivíduos específicos podem ser disponibilizados apenas aos usuários autorizados.
A PMS reserva-se no direito de monitorar e/ou registrar o uso de toda atividade e qualquer informação gerada, armazenada ou disseminada relacionada com a TI dentro da instituição. Para tal, deverão ser implementados controles, trilhas de auditoria e registros de atividades em todos os pontos e sistemas que a PMS julgar necessários para prevenir e mitigar riscos, bem como instalar câmeras de videomonitoramento nas dependências de acesso comuns aos seus usuários.
Para fins de segurança e prevenção à fraude, A PMS reserva-se no direito de implementar sistemas de controle de acesso a estações de trabalho, servidores internos e externos, e-mail, Internet, dispositivos móveis ou sem fio e outros componentes da rede.
Os ativos críticos ou sensíveis devem ser armazenados em áreas seguras, protegidas por perímetro de segurança definido, com barreiras de segurança adequadas aos riscos identificados, bem como devem ter controle de acesso.
Todos os usuários dos sistemas de informação da PMS devem ser identificados. Os dados coletados e armazenados devem ser segmentados para aplicar controles específicos e cumprir a legislação de proteção de dados aplicável. As regras para armazenamento e tratamento de dados devem ser estabelecidas por documentos específicos em conformidade com a legislação pertinente. A necessidade da coleta de autorização, quando aplicável, deve ser informada ao usuário conjuntamente com as condições de tratamento em documento específico eletrônico.
Todo incidente que afete a segurança da informação deve ser comunicado a GES para análise.
As informações geradas pelos controles e sistemas de monitoramento podem ser usadas para identificar usuários e seus acessos, realizar inspeção dos arquivos na rede, da unidade de disco local ou em qualquer outro ambiente interno da rede da PMS.
Caso os usuários optem pelo uso de dispositivos pessoais para fins profissionais para realização de atividades da PMS dentro de suas instalações ou interagindo com seu ambiente lógico, estes equipamentos devem estar sujeitos a controle e auditoria pela PMS a seu critério, quando necessário, observando a legislação vigente.
A GES bloqueará o acesso do usuário que violar as regras referenciadas neste documento e comunicará a ocorrência ao Gerente da Área.
As violações ao contido nesta PSI PMS estão sujeitas a análises disciplinares que podem acarretar as sansões previstas por lei. O uso dos recursos da PMS para atividades ilícitas pelos colaboradores configurará motivo para a instauração de processo de demissão por justa causa.

12 Proteção de Dados Pessoais

Em atendimento à Lei Geral de Proteção de Dados Pessoais (LGPD), a PMS deve garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo seu ciclo de vida, sendo esta categoria de dados tratados em conformidade com a legislação vigente.
Todo tratamento de dados pessoais deve estar relacionado a uma finalidade específica e ser informada ao titular dos dados em conformidade com os artigos 6º, 7º e 11 da LGPD, que tratam dos princípios da necessidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e prestação de contas.
Nas consultas estatísticas, sempre que possível, a PMS utilizará o processo de anonimização, pseudonimização ou efetuará a remoção dos identificadores pessoais dos dados, substituindo-os por valores de marcadores de posição para proteger a privacidade pessoal e a confidencialidade dos dados.
A PMS deve fazer registro das operações que envolvam tratamento de dados pessoais, utilizar protocolos de criptografia na sua transmissão e armazenamento de dados pessoais, bem como implementar um sistema de gestão de dados pessoais e um plano de resposta à violação de dados pessoais.

13 Responsabilidades Específicas

13.1 Dos Usuários em Geral

Todos os usuários são responsáveis pelo cumprimento e zelo da segurança da informação. O usuário assume total responsabilidade por qualquer dano decorrente do descumprimento das diretrizes enunciadas na PSI PMS.
Os usuários devem adotar as seguintes práticas:

- Cumprir a PSI PMS, diretrizes e demais procedimentos de segurança da informação;
- Procurar orientação de seu supervisor no caso de dúvidas sobre operação dos sistemas e em relação a segurança da informação;
- Assinar o Termo de responsabilidade, expressando formalmente a consciência e a responsabilidade pelo cumprimento das diretrizes deste PSI PMS;
- Assegurar que os recursos técnicos sejam utilizados somente para fins profissionais autorizados e em benefício da instituição;
- Seguir a Lei Federal 13.709/2018 (LGPD), suas atualizações e normas aplicáveis;
- Notificar imediatamente ao Núcleo de Tecnologia da Informação (NTI) a que estiver vinculado, qualquer descumprimento ou violação da PSI PMS e/ou de incidentes que possam colocar em risco a PMS.

13.2 Dos Núcleos de TI da PMS

Os Gerentes e Gestores de TI da PMS devem zelar pelo ambiente informacional e pela segurança da informação, dentro de sua área de abrangência e atuação, através das seguintes práticas:

- Assegurar a implementação dos equipamentos, mecanismos, práticas e políticas necessários para a segurança da informação;
- Demonstrar conduta voltada a segurança da informação através do exemplo quando na orientação de colaboradores, prestadores de serviço, estagiários e outros que estejam sob sua gestão, no cumprimento da PSI PMS, normas e procedimentos advindos da área de Segurança da Informação;
- Garantir o acesso e disseminação do conhecimento da PSI PMS, diretrizes, normas e procedimentos nela estabelecidos;
- Submeter solicitação prévia de permissão de acesso à Gerência Especial de Segurança (GES) da COGEL/DITEC, relacionando e justificando os ativos de informação que serão disponibilizados a terceiros;
- Inserir nas disposições contratuais com prestadores de serviços, clientes, terceiros e parceiros que necessitem compartilhar informações da PMS, cláusulas sobre o conhecimento da PSI PMS, responsabilidades de segurança compartilhadas, e conformidade com a LGPD, todas elas extensivas aos colaboradores e prestadores de serviços das contratadas;
- Adaptar normas, processos, procedimentos e sistemas sob a sua responsabilidade para o fiel cumprimento da PSI PMS;
- Relatar imediatamente quaisquer incidentes e violações de segurança da informação à Gerência Especial de Segurança (GES) da COGEL/DITEC.

13.3 Dos Proprietários dos Ativos de Informação

O Proprietário do ativo de informação é o gestor ou coordenador de determinada área ou projeto da PMS a que o ativo está relacionado, sendo este o responsável por manter o conjunto de informações relacionadas sob o seu controle.

São atribuições dos Proprietários dos Ativos de Informação:

- Relacionar as funções desenvolvidas, permissões e privilégios de acesso necessários;
- Manter registros e controles atualizados das permissões de acesso concedida a usuários no banco de dados de usuários dos sistemas envolvidos;
- Revogar o acesso ou alterar as permissões concedidas de acordo com a necessidade;
- Remover o acesso de usuários que não pertencem mais ao quadro de colaboradores do setor operacional do sistema;
- Cumprir e fazer cumprir os regulamentos e a legislação relativa à proteção de dados pessoais;
- Manter-se informado sobre a PSI PMS e solicitar informações sobre procedimentos de segurança da informação à área da Segurança da Informação da COGEL/DITEC em caso de necessidade.

13.4 Da Diretoria Técnica da COGEL – (COGEL/DITEC)

A Diretoria Técnica da Companhia de Governança Eletrônica de Salvador (COGEL/DITEC) é a responsável por administrar as capacidades operacionais dos recursos disponíveis na PMS voltados para a Tecnologia da Informação e Comunicação (TIC) e da Segurança da Informação.

As capacidades operacionais envolvem a governança, gerenciamento de ativos, proteção da informação, segurança de recursos humanos, segurança física do DATACENTER, segurança de sistemas e redes, Segurança de aplicativos, configuração de indicadores, gestão de identidade e de acesso, gerenciamento de ameaças e vulnerabilidades, continuidade dos negócios, segurança de relacionamento com fornecedores, conformidade, tratamento de incidentes e de ações voltadas para a continuidade dos negócios e de recuperação de desastres.

A COGEL/DITEC deve contar com uma equipe de profissionais responsáveis por identificar riscos, implementar medidas preventivas, disseminar diretrizes e práticas para o bom funcionamento dos ativos informacionais e zelar pela normalidade dos serviços de TIC desenvolvidos na PMS.

É atribuição da COGEL/DITEC também a elaboração de normas referentes a utilização dos ativos de informação e dos recursos computacionais relativos ao uso da Internet, acesso aos recursos de TIC, acesso e utilização do correio eletrônico, gerenciamento da auditoria de Segurança da Informação, gerenciamento de riscos, segurança em terceirização e prestação de serviços relacionados à Segurança da Informação.

Cabe ainda à COGEL/DITEC:

- Propor atualizações da PSI PMS e demais planos para submissão ao Comitê Consultivo de Segurança (CCS);
- Propor e apoiar iniciativas que visem promover a segurança da informação e dos ativos de informação da PMS;
- Elaborar, através de suas gerências subordinadas, ações voltadas à segurança da informação;
- Propor diretrizes, regras de conduta e adequação dos recursos técnicos e de infraestrutura necessários para atender a LGPD;
- Indicar um encarregado pela Proteção de Dados Pessoais no âmbito da PMS;
- Manter comunicação efetiva com o Comitê Consultivo de Segurança da Informação sobre incidentes e riscos que tenham potencial para afetar os negócios da PMS.

13.5 Da Gerência Especial de Segurança da COGEL (COGEL/GES)

A Gerência Especial de Segurança (GES) é a responsável por gerenciar os recursos operacionais disponíveis na PMS voltados para a Segurança da Informação.

Cabe ainda à GES:

- Supervisionar os recursos disponibilizados pela PMS para proteção e segurança da Informação;
- Atender a apoiar demandas relativas à segurança da informação;
- Propor a COGEL/DITEC medidas que visem promover a segurança da informação, incluindo sugestões relativas a PSI e demais planos correlatos;
- Elaborar e implementar o Plano Operacional de Segurança da Informação;
- Propor material didático e informativo para a disseminação de conhecimento em segurança da informação para colaboradores da PMS;
- Propor metodologias e processos específicos para a Segurança da Informação;
- Apoiar na avaliação e a adequação dos controles específicos da Segurança da Informação para sistemas ou serviços;
- Analisar e tratar incidentes de Segurança da Informação.

13.6 Do Comitê Consultivo de Segurança (CCS)

O Comitê Consultivo de Segurança (CCS) é uma estrutura matricial multidisciplinar que conta com a participação de gestores de diversas áreas da PMS. É formado por representantes das principais instâncias da instituição, incluindo a GSE.

O Comitê Consultivo se reúne semestralmente para tratar de assuntos relacionados com a segurança da informação. Reuniões adicionais podem ser realizadas sempre que for necessário para deliberar sobre alguma decisão relevante para a PMS.

É facultado ao CCS convocar ou consultar especialistas para tratar de algum assunto específico da área de Segurança da Informação.

São atribuições do CCS:

- Elaborar a Política de Segurança da Informação (PSI) e os seguintes planos de segurança: Plano Tático de Segurança da Informação, Plano de Gerenciamento de Vulnerabilidades, Plano de Resposta a Incidentes, Plano de Contingência e de Continuidade de Negócios e Plano de Recuperação de Desastres;
- Planejar, propor estratégias e avaliar riscos identificados;
- Recomendar investimentos relacionados à segurança da informação;
- Revisar a PSI PMS a qualquer tempo e, no mínimo, a cada 2 anos;
- Discutir e propor iniciativas para aprimorar a segurança da informação;
- Deliberar sobre a instauração de processos disciplinares em casos de descumprimento da PSI PMS.

13.7 Da Assessoria Jurídica da PMS

A PMS deve contar com apoio jurídico da Assessoria Jurídica para aconselhamento em questões que envolvam questões legislativas, regulatórias, litigiosas ou em questões que envolvam matéria específico do direito Digital, como a LGPD.

A Assessoria Jurídica da PMS tem as seguintes atribuições:

- Aconselhamento legal para questões jurídicas relacionadas com a Segurança da Informação;
- Acompanhar incidentes que necessitem conhecimento jurídico para resolução;
- Orientar formas de coletar e preservar evidências com o propósito de manter sua validade para uso em juízo;
- Sugerir minutas e analisar documentos relacionados a contratos de TI que envolvam a Segurança da Informação;

- Acompanhar processos disciplinares e respaldar juridicamente sansões e exceções, de acordo com a especificidade do caso;
- Sugerir alterações a PSI PMS e normas que envolvam a Segurança da Informação;
- Opinar sobre a regulamentação interna de segurança para que estejam em conformidade com a legislação vigente;
- Analisar e sugerir adequações em regulamentações internas ou contratos que necessitem se adequar a conformidade de alterações legislativas;
- Propor e/ou acompanhar demandas judiciais relacionadas a área de Segurança da Informação.

13.8 Da Gerência/Coordenação de Recursos Humanos

Cabe à Gerência/Coordenação de Recursos Humanos de cada órgão da PMS:

- Fornecer cópia da PSI PMS e acolher assinatura de consentimento no "Termo de Ciência e Aceitação de Responsabilidades" relativas à Segurança da Informação" em contratos individuais de trabalho na fase contratação de colaboradores e prestadores de serviços;
- Notificar o Núcleo Tecnologia da Informação (NTI) de seu órgão, as contratações, demissões ou mudança de cargo solicitando a revogação ou concessão de acessos aos sistemas corporativos da PMS;
- Tomar conhecimento, encaminhar e instaurar processos disciplinares envolvendo violações de políticas e normas de segurança da informação;
- Apoiar e promover conjuntamente com a Secretaria de Gestão (SEMGE) e com a Secretaria de Tecnologia (SEMIT), ações de conscientização e de capacitação em Segurança da Informação e Proteção de Dados Pessoais e da LGPD para os colaboradores da PMS.

14 Divulgação da PSI e Documentos Correlatos

Devem ser disponibilizados em portal online, no site da COGEL, a versão mais atualizada da Política de Segurança da Informação (PSI) e os documentos correlatos, a exemplo de modelos de documentos, formulários e anexos para operações com informações que envolvem empresas terceiras e demais contratados.

No Portal da COGEL, deverão ainda constar as informações de hierarquia e responsabilidades dos órgãos, setores e áreas técnicas que trabalham diretamente com a área de Segurança da Informação da PMS, de forma a facilitar e ampliar a comunicação dos clientes internos e externos.

Devem constar também as atribuições dos NTIs nas Secretarias e Órgãos no que concerne à Segurança da Informação, bem como os projetos na área tecnológica, para conhecimento público da PMS.

15 Disposições Gerais

A PMS se exonera de toda e qualquer responsabilidade perante o usuário, decorrente do seu uso indevido, negligente e/ou imprudente dos recursos e serviços concedidos.

A PMS reserva-se no direito de tomar as medidas administrativas e judiciais cabíveis contra os infratores, bem como analisar dados e evidências para a obtenção de provas a serem usadas em processos investigatórios e judiciais.

Toda e qualquer atividade que não esteja referenciada nesta PSI PMS ou em normativos específicos complementares devem ser realizados apenas após consulta e autorização do gestor responsável da área.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da PMS.

ANEXO II

SALVADOR PREFEITURA

Normas de Segurança da Informação

Documento de Normas Administrativas

COGEL/DITEC/GSE
V 1.0

Histórico de revisões

COGEL Companhia de Governança Eletrônica de Salvador	SALVADOR PREFEITURA	GSI
Normas de Segurança da Informação da PMS (NSI PMS)	*Versão: 1.0*	
	Data: 18/08/2023	
Para Divulgação	*COGEL/DITEC/GSE*	

Histórico de Versões	Data	Alteração
Versão 1.0	18/10/2023	Primeira versão da NSI PMS adequada a norma ISO/IEC 27002:2022 e ap+os acolhimento das sugestões do CCS

Sumário

1 Introdução 9
2 Norma 01 – Responsabilidades dos Órgãos 10
2.1 Objetivo 10
2.2 Definições 10
2.3 Abrangência 10
2.4 Competências 10
2.4.1 Diretoria Técnica (COGEL/DITEC) 10
2.4.2 Núcleos de Tecnologia da Informação (NTI) ou setores equivalentes dos órgãos e entidades: 11
2.5 Documentos Relacionados 12
2.6 Data de Revisão 12
3 Norma 02 - Classificação da Informação 12
3.1 Objetivo 12
3.2 Definições 12
3.3 Abrangência 13
3.4 Diretrizes 13
3.5 Recomendações para Classificação 14
3.6 Competência 14
3.7 Competências do Usuário 15
3.8 Autoridades competentes para classificação das informações 15
3.9 Proprietário da Informação 15
3.10 Documentos Relacionados 15
3.11 Data de Revisão 15
4 Norma 03 - Uso da Internet 16
4.1 Objetivo 16
4.2 Definições 16
4.3 Abrangência 16
4.4 Diretrizes 16
4.5 Controles de Acesso a Serviços da Internet 17
4.6 Conexões de Rede com a Internet 17
4.7 Uso Aceitável da Internet 18
4.8 Uso Corporativo de Mídias Sociais 19
4.9 Perfis Institucionais Mantidos pela PMS em Mídias Sociais 20
4.10 Criptografia 20
4.11 Legalidade 20
4.12 Download de Arquivos 21
4.13 Competências do Núcleo de Tecnologia da Informação do Órgão ou Entidade: 21
4.14 Documentos relacionados 21
4.15 Data de Revisão 21
5 Norma 04 - Acesso aos Recursos de Tecnologia da Informação 21
5.1 Objetivo 21
5.2 Definições 21
5.3 Abrangência 22
5.4 Concessão de Acesso 22
5.5 Conexão de Equipamentos 23
5.6 Gerenciamento de Senhas 23
5.7 Análise Crítica 24
5.8 Competências 24
5.8.1 do Núcleo de Tecnologia da Informação do Órgão ou Entidade 24
5.8.2 Das chefias dos setores 24
5.8.3 Usuário 24
5.9 Documentos Relacionados 24
5.10 Data de Revisão 25
6 Norma 05 - Acesso e Utilização do Correio Eletrônico 25
6.1 Objetivo 25
6.2 Definições 25
6.3 Abrangência 25
6.4 Diretrizes 25
6.5 Competências 26
6.5.1 Área de Tecnologia da Informação do Órgão ou Entidade 26
6.5.2 Chefia do setor do Usuário 27
6.5.3 Usuário 27
6.6 Documentos Relacionados 27
6.7 Data de Revisão 27
7 Norma 06 - Gerenciamento de Incidentes de Segurança da Informação 27
7.1 Objetivo 27
7.2 Definições 27
7.3 Abrangência 27
7.4 Diretrizes 28
7.5 Competências 28
7.5.1 Área de Tecnologia da Informação do Órgão ou Entidade: 28
7.5.2 Gestor da Área do Usuário 28
7.5.3 Usuário 28
7.6 Documentos Relacionados 28
7.7 Data de Revisão 29
8 Norma 07 - Gerenciamento da Auditoria de Segurança da Informação 29
8.1 Objetivo 29
8.2 Definições 29
8.3 Abrangência 29
8.4 Diretrizes 29
8.5 Competências 30
8.5.1 Auditor 30
8.5.2 Áreas de Negócio do Órgão ou Entidade 31
8.6 Documentos Relacionados 31
8.7 Data de Revisão 31
9 Norma 08 - Gestão de Continuidade de Negócios 31
9.1 Objetivo 31
9.2 Definições 31
9.3 Abrangência 32
9.4 Diretrizes 32
9.5 Competências 33
9.5.1 Alta Administração do Órgão ou Entidade 33
9.5.2 Gestores das Áreas de Negócio do Órgão ou Entidade 33
9.5.3 Usuários 33
9.6 Documentos Relacionados 33
9.7 Data de Revisão 33
10 Norma 09 - Gestão de Riscos 33
10.1 Objetivo 33
10.2 Definições 34
10.3 Abrangência 34
10.4 Diretrizes 34
10.5 Definição do Contexto de Riscos 34
10.6 Análise de Riscos 34
10.7 Avaliação de Riscos 35
10.8 Tratamento e Comunicação de Riscos 35
10.9 Competências 35
10.9.1 Alta Administração do Órgão ou Entidade 35
10.9.2 Áreas de Negócio do Órgão ou Entidade 36
10.9.3 Área de Tecnologia da Informação do Órgão ou Entidade 36
10.10 Documentos Relacionados 36
10.11 Data de Revisão 36
11 Norma 10 - Contabilização de Ativos de Tecnologia da Informação 36
11.1 Objetivo 36
11.2 Definições 36
11.3 Abrangência 37
11.4 Diretrizes 37
11.5 Competências 38
11.5.1 Área de Tecnologia da Informação do Órgão ou Entidade 38
11.5.2 Usuário 38
11.6 Documentos Relacionados 38
11.7 Data de Revisão 38
12 Norma 11 - Intercâmbio de Informações 38
12.1 Objetivo 38
12.2 Definições 38
12.3 Abrangência 39
12.4 Diretrizes 39
12.5 Mídias em Trânsito 40
12.6 Competências 40
12.6.1 Área de Tecnologia da Informação do Órgão ou Entidade 40
12.6.2 Usuário 40
12.7 Documentos Relacionados 40
12.8 Data de Revisão 40
13 Norma 12 - Segurança Física 40
13.1 Objetivo 40
13.2 Definições 40
13.3 Abrangência 41
13.4 Diretrizes 41
13.5 Em Áreas Protegidas 41
13.6 Em Áreas Seguras 41
13.7 Controles de Entrada Física 42
13.8 Segurança em Escritórios, Salas e Instalações de Processamento 42
13.9 Trabalho em Áreas Seguras 42
13.10 Instalação e Proteção dos Equipamentos 43
13.11 Competências 43
13.11.1 Área de Tecnologia da Informação do Órgão ou Entidade 43
13.11.2 Usuário 44
13.12 Documentos Relacionados 44
13.13 Data de Revisão 44
14 Norma 13 - Segurança em Terceirização e Prestação de Serviços 44
14.1 Objetivo 44
14.2 Definições 44
14.3 Abrangência 44
14.4 Diretrizes 44
14.5 Competências 46
14.5.1 Áreas de Negócio do Órgão ou Entidade 46

14.5.2 Área de Tecnologia da Informação do Órgão ou Entidade 46
14.6 Documentos Relacionados 46
14.7 Data de Revisão 46
15 Norma 14 - Desenvolvimento e Manutenção de Aplicações 46
15.1 Objetivo 46
15.2 Definições 46
15.3 Abrangência 47
15.4 Diretrizes 47
15.5 Desenvolvimento Terceirizado 49
15.6 Testes 49
15.7 Aceitação de Software 50
15.8 Mudanças Técnicas no Ambiente de Produção 50
15.9 Implantação 50
15.10 Competências 50
15.10.1 Áreas de Negócio do Órgão ou Entidade: 50
15.10.2 Área de Tecnologia da Informação do Órgão ou Entidade 51
15.11 Documentos Relacionados 51
15.12 Data de Revisão 51
16 Norma 15 - Distribuição de Hardware e Software 51
16.1 Objetivo 51
16.2 Definições 51
16.3 Abrangência 52
16.4 Aquisição de Hardware e Software 52
16.5 Distribuição de Hardware e Software 52
16.6 Competências 53
16.6.1 Áreas de Negócio do Órgão ou Entidade 54
16.6.2 Área de Tecnologia da Informação do Órgão ou Entidade: 54
16.7 Documentos Relacionados 54
16.8 Data de Revisão 54
17 Norma 16 - Proteção Contra Código Malicioso 54
17.1 Objetivos 54
17.2 Definições 54
17.3 Abrangência 55
17.4 Diretrizes 55
17.5 Competências 56
17.5.1 Área de Tecnologia da Informação do Órgão ou Entidade 56
17.5.2 Usuário 56
17.6 Documentos Relacionados 56
17.7 Data de Revisão 56

18 Norma 17 - Uso de Dispositivos Móveis 56
18.1 Objetivo 56
18.2 Definições 56
18.3 Abrangência 58
18.4 Diretrizes 58
18.5 Acesso à Internet 58
18.6 Uso Adequado de Dispositivos Móveis Corporativos 59
18.7 Uso de dispositivo móveis de propriedade particular 59
18.8 Usuários visitantes com dispositivos móveis 60
18.9 Termo de Uso e Responsabilidade 60
18.10 Competências 60
18.10.1 Área de Tecnologia da Informação do Órgão ou Entidade 60
18.10.2 Gestor da Área do Usuário 61
18.10.3 Usuários 61
18.11 Documentos relacionados 61
18.12 Data de Revisão 61

1 Introdução

A COGEL/DITEC, através da Assessoria de Segurança Cibernética e da Gerência Especial de Segurança (GES) são as responsáveis por gerenciar os recursos disponíveis na PMS voltados para a Segurança da Informação e as suas capacidades operacionais.

Medidas devem ser aplicadas para prover garantias às informações, buscando resguardar aqueles que são considerados os principais pilares da Segurança da Informação: Confidencialidade: toda informação, esteja ela em meio eletrônico ou não, deve estar acessível somente a quem tem o direito a este acesso. Mecanismos de processos e tecnologia devem ser implementados buscando satisfazer esta premissa; Integridade: toda informação trafegada ou armazenada deve ter garantias quanto à sua integridade, assegurando que ela não seja indevidamente alterada ou eliminada; Disponibilidade: as informações devem estar sempre disponíveis para os usuários que dela necessitarem e que tenham autorização para tal acesso; Autenticidade: devem ser adotados mecanismos que garantam a autenticidade e rastreabilidade dos usuários na utilização dos recursos computacionais, de forma a tornar possível a identificação dos autores de qualquer ação que seja feita utilizando os sistemas informatizados e meios de comunicação.

A norma NBR ISSO/IEC 27001:2022 , em conformidade com a legislação vigente no Brasil e com base nas recomendações da ABNT NBR ISO / IEC 27002:2022, orientam procedimentos para a Gestão da Segurança da Informação através da implementação dos seguintes controles de segurança da informação, incluindo as Normas de Segurança da Informação, que devem estar disponíveis a todos para orientar a boa utilização dos recursos de TI e garantir a segurança da Informação.

Para assegurar todos estes aspectos, é necessário que seja colocado em prática um processo de gestão de segurança da informação. Este processo, baseado na Norma ISO/IEC 27001:2022 ("Information Technology - Security Techniques - Information Security Management Systems - Requirements"), é o chamado SGSI - Sistema de Gestão de Segurança da Informação (em inglês, ISMS - Information Security Management System). O SGSI prevê diversas ações, subprocessos, Normas e Procedimentos de Segurança, praticando a missão de reduzir continuamente os riscos à segurança das informações e aos ativos críticos de uma Organização.

Um dos componentes mais importantes do processo de Gestão de Segurança da Informação é o conjunto de Normas de Segurança da Informação que irá guiar os gestores e usuários na produção, manuseio e guarda das informações da Organização. Este documento traz um conjunto básico de normas a serem implantadas pelos órgãos e entidades da Administração Pública Municipal, buscando elevar o nível de Segurança da Informação na Prefeitura Municipal de Salvador (PMS).

2 Norma 01 – Responsabilidades dos Órgãos

2.1 Objetivo

Orientar todos os órgãos e entidades da Administração Pública Municipal, quanto à utilização das Normas de Segurança da Informação.

2.2 Definições

Ativos de Tecnologia da Informação: estações de trabalho, servidores, softwares, mídias e quaisquer equipamentos eletrônicos relacionados à Tecnologia da Informação, bem como processos, pessoas e ambientes.

Gestão de Continuidade de Negócios: processo de gestão que identifica ameaças em potencial e os possíveis impactos às operações de negócio caso essas ameaças se concretizem. Este processo fornece um framework para que se construa uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar a reputação e a marca do órgão ou entidade e suas atividades de valor agregado.

Gestão de Riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos, incluindo, inclusive, análise, avaliação, tratamento, aceitação e comunicação dos riscos.

Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio.

Segurança da Informação: conjunto de processos articulados, que busca a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e ampliar as oportunidades de negócio.

2.3 Abrangência

Esta Norma e todas as outras Normas contidas neste documento se aplicam a todos os órgãos e entidades da Administração Pública Municipal.

2.4 Competências

2.4.1 Diretoria Técnica (COGEL/DITEC)

- gerenciar as atividades e projetos de Segurança da Informação;
- propor ao Comitê Consultivo de Segurança da Informação (CCS) estratégias, programas, planos, projetos e normas de Segurança da Informação;
- coordenar ações de Segurança da Informação que envolvam os órgãos e entidades da Administração Pública Municipal;

- mobilizar a alta administração e os gestores dos órgãos e entidades da Administração Pública Municipal para o cumprimento da Política de Segurança da Informação da PMS (PSI PMS) e a participação destes na implementação de soluções de segurança.
- apreciar e validar as proposições do CCS, referentes às normas e políticas de Segurança da Informação na Administração Pública Municipal:
- apreciar matérias que subsidiem o estabelecimento de políticas e estratégias para a Segurança da Informação da Administração Pública Municipal;
- difundir e promover o cumprimento das metodologias e boas práticas em Segurança da Informação;
- divulgar os principais aspectos da Segurança da Informação;
- avaliar as informações sobre monitoramento do ambiente tecnológico dos órgãos e entidades da Administração Pública Municipal e incidentes detectados pela COGEL;
- desenvolver, definir e divulgar indicadores de Segurança da Informação;
- acompanhar e avaliar os indicadores de Segurança da Informação definidos para Administração Pública Municipal;
- consolidar e emitir os relatórios de incidentes de Segurança da Informação dos órgãos e entidades;
- analisar informações de incidentes de Segurança da Informação;
- propor ações para tratamento de incidentes de Segurança da Informação e mitigação de riscos;
- avaliar as informações sobre o monitoramento do ambiente tecnológico e incidentes de Segurança da Informação detectados pela COGEL.
- propor adoção de soluções de Segurança da Informação existentes no mercado;
- capacitação na operacionalização da ferramenta de gestão de riscos para a Segurança da Informação;
- analisar e dirimir dúvidas sobre as normas e casos omissos.

2.4.2 Núcleos de Tecnologia da Informação (NTI) ou setores equivalentes dos órgãos e entidades:

- Orientar atividades de Segurança da Informação no âmbito de seu órgão vinculado;
- acompanhar, periodicamente, a evolução dos indicadores de Segurança da Informação adotados no âmbito do respectivo órgão a que está subordinado;
- apoiar, sugerir, garantir e implementar em sua área de atuação, as ações de Segurança da Informação estabelecidas pela PMS;
- cumprir a Política de Segurança da Informação da PMS (PSI PMS) e as Normas de Segurança da Informação da PMS (NSI PMS);
- reportar a ocorrência de incidentes de Segurança da Informação ao superior imediato do órgão vincluado com cópia para a Gerência de Segurança da Informação da Companhia de Governança Eletrônica de Salvador (COGEL/DITEC/GSE).
- Para a execução das atividades de Segurança da Informação, os órgãos e entidades da Administração Pública Municipal deverão observar todas as normas disponibilizadas neste documento.

2.5 Documentos Relacionados

Política de Segurança da Informação da PMS (PSI PMS)

ABNT NBR ISO/IEC 27002:2022

2.6 Data de Revisão

18/10/2023

3 Norma 02 - Classificação da Informação

3.1 Objetivo

Estabelecer diretrizes que garantam que todas as informações, independente de seus meios de armazenamento ou transmissão, recebam níveis adequados de proteção e sejam classificadas com clara indicação do assunto, fundamento da classificação, indicação do prazo do sigilo e identificação da autoridade que a classificou, respeitando o princípio da observância da publicidade como preceito geral e do sigilo como exceção, conforme a Lei Federal nº 12.527, de 18 de Novembro de 2011 (Lei de Acesso à Informação Pública).

3.2 Definições

Custodiante da Informação: aquele que armazena, processa, veicula e trata a informação, mediante orientação dada pela classificação da informação e assume, em conjunto com o proprietário da informação, a responsabilidade pela proteção desta.

Documento: unidade de registro de informações, qualquer que seja o suporte ou formato. Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informação Pessoal: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem.

Informação Sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Proprietário da Informação: aquele que gera ou adquire a informação.

Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

3.3 Abrangência

Esta Norma se aplica a todos os usuários das informações custodiadas ou de propriedade da Administração Pública Municipal.

3.4 Diretrizes

3.4.1. A informação em poder dos órgãos e entidades, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Município, poderá ser classificada no grau Ultrassecreto, Secreto ou Reservado.

3.4.2. Para a classificação da informação em grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:

3.4.2.1. a gravidade do risco ou dano à segurança da sociedade e do Município;

3.4.2.2. o prazo máximo de classificação em grau de sigilo ou o evento que defina seu termo final.

3.4.3. Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista, devem vigorar, a partir da data de sua produção, nos seguintes parâmetros:

3.4.3.1. Ultrassecreta: 25 (vinte e cinco) anos;

3.4.3.2. Secreta: 15 (quinze) anos;

3.4.3.3. Reservada: 5 (cinco) anos.

3.4.4. O prazo de sigilo das informações classificadas no grau Ultrassecreto poderá ser prorrogado por uma única vez e por período determinado não superior a vinte e cinco anos, enquanto seu acesso ou divulgação puder ocasionar ameaça externa à integridade do território nacional ou grave risco às relações internacionais do Município.

3.4.5. As informações que puderem colocar em risco a segurança do Prefeito e Vice-prefeito do Município de Salvador e respectivos cônjuges e filhos (as) deverão ser, automaticamente, consideradas como reservadas e ficar sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição.

3.4.6. As informações que não forem classificadas como Ultrassecretas, Secretas ou Reservadas deverão ser consideradas, automaticamente, como públicas, resguardadas as exceções legalmente previstas como sigilo, a exemplo de:

3.4.6.1. sigilo fiscal, bancário, de operações e serviços no mercado de capitais, comercial, profissional, industrial e segredo de justiça;

3.4.6.2. informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

3.4.6.3. Transcorrido o prazo de classificação ou consumado o evento que defina o seu termo final, a informação deverá ser considerada automaticamente classificada como pública, respeitadas as exceções previstas nesta norma.

3.5 Recomendações para Classificação

3.5.1. Informação "pessoal" não é considerada uma classificação, mas uma designação para uma informação relacionada à pessoa natural identificada ou identificável relativa à intimidade, vida privada, honra e imagem, significando que a informação é direcionada e que somente o destinatário e as pessoas expressamente autorizados por ele podem ter acesso.

3.5.2. Toda informação deve possuir um rótulo com a sua classificação. As informações não rotuladas serão classificadas, automaticamente, como “Públicas”, ressalvadas as exceções previstas nesta norma.

3.5.3. A classificação das informações deve ser feita para determinar as medidas de proteção necessárias, visando atender as diretrizes da Lei de Acesso à Informação Pública e otimizar os custos com a sua proteção e disponibilização.

3.5.4. A classificação deve ser realizada quando a informação é gerada ou adquirida, conforme as seguintes competências:

3.5.4.1. **Grau Ultrassecreto:** Prefeito e Vice-prefeito;

3.5.4.2. **Grau Secreto:** Além dos previstos no item 3.5.4.1 também, os Secretários Municipais, as autoridades com as mesmas prerrogativas, os titulares máximos de autarquias, fundações ou empresas públicas e sociedades de economia mista.

3.5.4.3. **Grau Reservado:** Além dos previstos nos itens 3.5.4.1 e 3.5.4.2, também aqueles que exerçam funções de direção, comando ou chefia, no Grau 57 ou superior, do Grupo-Direção e Assessoramento Superior ou hierarquia equivalente, de acordo com regulamentação específica de cada órgão ou entidade.

3.6 Competência

3.6.1. A competência prevista nos itens 3.5.4.1 e 3.5.4.2 poderá ser delegada expressamente pela autoridade responsável a agente público, inclusive em missão no exterior, vedada a subdelegação.

3.6.2. O proprietário da informação pode solicitar apoio técnico à COGEL, através da Diretoria Técnica (DITEC), caso existam dificuldades ou dúvidas acerca da classificação a ser dada a uma informação.

3.6.3. A informação deve receber tratamento adequado à sua classificação durante todo o seu ciclo de vida.

3.6.4. A inexistência de classificação explícita não exime o proprietário, os custodiantes e os usuários das suas responsabilidades quanto a avaliar o nível de sensibilidade da informação.

3.6.5. Os órgãos e entidades da Administração Pública Municipal deverão reavaliar as informações classificadas no grau Ultrassecreta e Secreto, no prazo máximo de dois anos. Enquanto não transcorrido o prazo de reavaliação previsto, será mantida a classificação da informação, observados os prazos e disposições desta norma. As informações classificadas

no grau Ultrassecreto e Secreto não reavaliadas no prazo previsto de dois anos serão consideradas, automaticamente, de acesso público.

3.6.6. As informações classificadas no grau Ultrassecreto, Secreto e Reservado deverão conter:

- código de indexação de documento;
- categoria na qual se enquadra a informação;
- indicação de dispositivo legal que fundamenta a classificação;
- data da produção, data da classificação e prazo da classificação.

3.6.7. É expressamente proibida aos usuários a utilização, repasse e/ou divulgação indevida de toda e qualquer informação de propriedade da Administração Pública Municipal, exceto nas hipóteses previstas na Lei Federal nº 12.527, de 18 de novembro de 2011.

3.6.8. Antes que informações custodiadas ou de propriedade da Administração Pública Municipal sejam disponibilizadas a terceiros, estes devem ser orientados e supervisionados quanto aos aspectos da segurança da informação.

3.6.9. A Administração Pública Municipal deve garantir que o compromisso de sigilo seja parte integrante dos contratos firmados com terceiros.

3.6.10. Informações Reservadas, Secretas ou Ultrassecretas não devem ser descartadas como lixo comum.

3.6.11. Documentos impressos ou em mídia eletrônica, que contenham informação com esses níveis de classificação, devem ser destruídos antes de serem descartados, de forma que torne impossível a sua recuperação.

3.7 Competências do Usuário

Aplicar o tratamento adequado à informação, de acordo com os níveis definidos nesta norma.

3.8 Autoridades competentes para classificação das informações

Classificar as informações, conforme as diretrizes desta norma.

3.9 Proprietário da Informação

Determinar o nível de criticidade e a classificação correta das informações utilizadas nos ativos sob sua responsabilidade, de forma a subsidiar as decisões de classificação a serem aplicadas pelos entes competentes.

3.10 Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2022
- Lei Federal de Acesso à Informação Pública – (Lei Federal nº 12.527, de 18 de novembro de 2011).

3.11 Data de Revisão

18/10/2023

4 Norma 03 - Uso da Internet

4.1 Objetivo

Estabelecer as diretrizes de proteção relativas ao uso da Internet e de outras redes públicas de computadores, com o objetivo de reduzir o risco a que estão expostos os Ativos de Tecnologia da Informação da Administração Pública Municipal, tendo em vista que a Internet tem sido veículo de muitas ações prejudiciais às organizações, gerando perdas financeiras, perdas de produtividade, danos aos sistemas e à imagem da organização, entre outras consequências.

4.2 Definições

Ativos de Tecnologia da Informação: estações de trabalho, servidores, softwares, mídias e quaisquer equipamentos eletrônicos relacionados à Tecnologia da Informação, bem como processos, pessoas e ambientes.

Criptografia: técnica utilizada para tornar a informação original ilegível, permitindo que somente o destinatário (detentor da chave de criptografia) a decifre.

Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio.

Internet: consiste em milhares de redes de computadores interconectadas mundialmente e que pela sua abrangência e facilidade de uso, tem sido usada como plataforma para a prestação de um crescente número de serviços.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

Mídias Sociais: são plataformas baseadas em Internet que disponibilizam informações, notícias e quaisquer tipos de conteúdo, que permitem a interação entre pessoas, possibilitando o compartilhamento de imagens, vídeos, experiências, pensamentos, entre outros.

4.3 Abrangência

Esta Norma se aplica a todos os usuários que fazem uso da Internet, permanente ou temporariamente, através dos recursos computacionais disponibilizados pela Administração Pública Municipal, bem como os que utilizam a Internet como meio de comunicação através de conexão com a rede interna do Município.

4.4 Diretrizes

4.4.1. Toda área de transferência de dados em computadores da Administração Pública Municipal acessível pela Internet e disponível publicamente para gravação deve ser limpa regularmente.

4.4.2. A informação obtida na Internet de forma livre e gratuita deve ser confirmada por fontes fidedignas antes de ser efetivamente usada.

4.4.3. A Administração Pública Municipal pode examinar, sem aviso prévio, o conteúdo de cache de navegadores Web, favoritos, histórico de sites visitados, configurações dos softwares e outras informações armazenadas ou transmitidas pelos seus computadores.

4.4.4. Os Ativos de Tecnologia da Informação da Administração Pública Municipal, incluindo as conexões com a Internet, hardware e software, devem ser empregados na consecução dos seus objetivos, sendo vedada a sua utilização para outros fins, exceto para os casos explicitamente permitidos por esta norma.

4.5 Controles de Acesso a Serviços da Internet

4.5.1. A permissão de acesso à Internet deve ser seletiva em relação aos serviços disponibilizados e ser concedida exclusivamente àqueles usuários que necessitem deste acesso para o seu trabalho, podendo ser removida quando não for mais necessária.

4.5.2. O acesso à Internet deve ser disponibilizado por meio de listas positivas ou negativas, cabendo a cada unidade definir suas regras.

4.5.3. A permissão de acesso à Internet deve ser concedida através de uma Conta de Usuário que possibilite identificar, individualmente, seu proprietário, podendo o histórico de acesso, inclusive o conteúdo, ser monitorado, sem necessidade de notificação prévia, devendo ser armazenado por um período mínimo de 90 (noventa) dias, ou quando cabível, por período previsto em lei.

4.5.4. Não é permitido suprimir, omitir ou mascarar a identificação da Conta de Usuário a qualquer serviço da Internet, exceto para os serviços que permitem apenas conexão anônima, não sendo permitido também o uso de mecanismos de dissimulação do usuário, como remailers, IP Spoofing e tradutores de URL.

4.5.5. A Administração Pública Municipal pode, sem aviso prévio, restringir o acesso a serviços da Internet, tais como sítios Web, redes de dados ponto a ponto e download de arquivos.

4.5.6. A possibilidade de acessar qualquer serviço da Internet não implica em autorização para acessá-lo.

4.6 Conexões de Rede com a Internet

4.6.1. É vedada a conexão entre qualquer rede de dados da Administração Pública Municipal e a Internet através de serviços de telecomunicações não autorizados pela área de TIC do órgão ou entidade.

4.6.2. É vedada a utilização de dispositivos de acesso à Internet não autorizados pela área de Tecnologia da Informação dos órgãos ou entidades, em equipamentos pertencentes à Administração Pública Municipal.

4.6.3. Toda comunicação entre computadores remotos e as redes da Administração Pública Municipal, através da Internet ou outra rede pública, deve ser autenticada e criptografada, usando soluções tecnológicas autorizadas pelo órgão ou entidade responsável pela rede, com exceção do acesso aos sítios Web públicos da Administração Pública Municipal.

4.6.4. Toda a comunicação entre as redes da Administração Pública Municipal e a Internet ou qualquer outra rede pública deve necessariamente passar por firewall, configurado com política restritiva, com monitoramento bidirecional dos fluxos de comunicação e com proteção contra-ataques cibernéticos.

4.7 Uso Aceitável da Internet

4.7.1. É permitido o uso de mídias sociais, cabendo a cada unidade definir suas regras de acesso.

4.7.2. É permitido o acesso a sites que sejam fontes de informação necessária à execução das atividades da Administração Pública Municipal.

4.7.3. É permitido o uso de serviços pessoais prestados através da Internet, tais como banco on-line, reservas de passagens, serviços de órgãos públicos, entre outros, limitados ao estritamente necessário, nos horários estabelecidos pelas áreas de Tecnologia da Informação dos órgãos e entidades da Administração Pública Municipal.

4.7.4. O uso de serviço de mensagem instantânea deve ser preferencialmente realizado por meio da ferramenta corporativa.

4.7.5. Não devem ser usados os recursos de “Salvar Senha” ou “Lembrar Senha”, disponíveis na maioria das aplicações (Outlook, Internet Explorer etc.), devendo ser desmarcada sempre que for apresentada esta opção.

4.7.6. Senhas não devem ser incluídas em nenhum outro processo de autenticação automática disponível.

4.7.7. Quando estiver usando a Internet e verificar que o site acessado contém conteúdo impróprio, o usuário deve abandonar o site e abrir um incidente de Segurança da Informação.

4.7.8. Não é permitido o uso de aplicações ponto a ponto (peer-to-peer) para distribuição de arquivos.

4.7.9. Não é permitido o uso de jogos on-line.

4.7.10. Ressalvados os interesses da Administração Pública Municipal, não é permitido:

4.7.10.1. o acesso e/ou a publicação de conteúdos impróprios, que são aqueles relativos à pornografia, racismo, violência, incitação ao ódio, invasão de computadores, jogos, entre outros;

4.7.10.2. o uso de serviços de mensagem instantânea, seja por software específico ou via Web;

4.7.10.3. o uso de serviços de áudio e vídeo em tempo real, tais como rádio online, TV on-line e telefonia IP;

4.7.10.4. a sondagem, investigação ou teste de vulnerabilidade em computadores e sistemas da Administração Pública Municipal ou de qualquer outra organização, exceto quando autorizada pela área de Tecnologia da Informação do respectivo órgão ou entidade da Administração Pública;

4.7.10.5. o uso ou a posse de ferramentas de hardware e software para sondagem, análise de vulnerabilidade, monitoramento de rede, comprometimento de sistemas, ataques e captura de dados, exceto quando autorizado pela área de Tecnologia da Informação do respectivo órgão ou entidade da Administração Pública Municipal.

4.8 Uso Corporativo de Mídias Sociais

4.8.1. Regras básicas de boa convivência, de educação, adotadas dentro do órgão ou entidade, também são válidas para ambientes virtuais;

4.8.2. Participar de mídias sociais é um ato de caráter público. O usuário será responsável por tudo que publicar, compartilhar, curtir, comentar, entre outros, devendo estar ciente que na Internet tudo fica registrado podendo ser rastreado;

4.8.3. Quando utilizadas para fins profissionais, é recomendável prudência em relação ao conteúdo publicado e compartilhado;

4.8.4. Não é permitido:

4.8.4.1. Criar perfis com nomes que façam menção ao órgão ou entidade e ao Governo Público Municipal sem autorização da Assessoria de Comunicação, ou unidade equivalente;

4.8.4.2. Falar em nome do órgão ou entidade, a não ser que seja autorizado oficialmente;

4.8.4.3. Vincular sua conta de e-mail corporativo a contas pessoais em mídias sociais;

4.8.4.4. Responder a ataques ou provocações nas mídias sociais envolvendo o nome do órgão/entidade. Neste caso, o colaborador deve informar o fato ao gestor imediato ou à Assessoria de Comunicação;

4.8.4.5. Fazer qualquer tipo de manifestação ou emitir opinião que possa ser considerada ambígua, discriminatória, caluniosa, difamatória, agressiva ou hostil;

4.8.4.6. Divulgar informações classificadas como sigilosa ou internas para o órgão/entidade, ou sobre a vida pessoal de colaboradores;

4.8.4.7. Participar de grupos ou discussões relacionadas a assuntos de cunho negativo ao órgão/entidade e ao local de trabalho;

4.8.4.8. Emitir opinião negativa ou publicar mensagens de conteúdo ofensivo, ou moralmente questionável, sobre qualquer área ou colaboradores do órgão/entidade;

4.8.4.9. Postar ou emitir manifestações partidárias, como endosso a campanhas políticas, declarar apoio a partidos políticos ou políticos de qualquer partido.

4.9 Perfis Institucionais Mantidos pela PMS em Mídias Sociais

4.9.1. No intuito de preservar a imagem institucional da PMS, garantindo segurança, transparência e lisura na comunicação nos serviços prestados pela prefeitura, a padronização dos perfis institucionais mantidos pela PMS facilita os usuários e cidadãos a identificarem páginas e sistemas web legítimos evitando que estes usuários sejam vítimas de crimes cibernéticos.

4.9.2. Toda a comunicação, em meios digitais deverá ser exercida por órgão competente e por somente ele, com apoio e chancela da COGEL/DITEC, que deverá avaliar os riscos eminentes de uso das plataformas que ofereçam este serviço.

4.9.3. As informações para criação de perfis institucionais da PMS em redes sociais devem ser documentadas e conter, no mínimo, as seguintes informações: perfil criado, credenciais, plataforma, data e hora, objetivo, validade, autor, solicitante e órgão responsável.

4.9.4. Os perfis institucionais da PMS, criados em mídias sociais, tem por objetivo único e restrito, promover a divulgação junto a sociedade de ações, serviços e campanhas que visem a informação e o bem-estar da população.

4.9.5. Caberá aos órgãos responsáveis pelos perfis institucionais da PMS, nas redes sociais e plataformas digitais, o seu respectivo monitoramento, de forma a garantir a sua legitimidade e segurança da instituição.

4.10 Criptografia

4.10.1. Recomenda-se que toda a informação classificada como sigilosa, transmitida pela Internet, deve ser criptografada, conforme padrões de criptografia homologados pela área de Tecnologia da Informação do respectivo órgão ou entidade da Administração Pública Municipal.

4.10.2. Informações que são alvo típico de criminosos, tais como senhas de contas bancárias, números de cartões de crédito, senhas de sistemas, entre outras, não devem ser publicadas na Internet ou transmitidas via Correio Eletrônico sem criptografia.

4.11 Legalidade

4.11.1. Sempre que as transações através da Internet ultrapassarem as fronteiras nacionais, devem ser observadas as legislações internacionais pertinentes.

4.11.2. A propriedade intelectual deve ser respeitada em qualquer atividade e sempre que os recursos computacionais da Administração Pública Municipal estiverem sendo usados.

4.11.3. A reprodução ou encaminhamento de qualquer conteúdo protegido por direitos de propriedade requer a autorização do proprietário dos direitos autorais.

4.11.4. Sempre que informações obtidas da Internet forem usadas em documentos internos, a fonte deve ser citada.

4.11.5. A indicação de direitos reservados deve ser presumida para todo conteúdo disponível na Internet, a menos que contenha informação contrária.

4.11.6. Usuários dos serviços de Internet da Administração Pública Municipal não devem obter, armazenar ou transmitir conteúdo ilegal, tais como software não licenciado, pornografia infantil, senhas, informações bancárias extraviadas, entre outros.

4.12 Download de Arquivos

4.12.1. Não é permitido o download de filmes, músicas, vídeo clips ou conteúdos semelhantes relacionados a entretenimento, ressalvado os interesses da Administração Pública Municipal, desde que eles não sejam protegidos por direitos autorais.

4.12.2. O download de arquivos com grande volume de dados (acima de 1 Tb ou com duração acima de 1 hora) deve considerar as limitações da conexão com a Internet (casos em que os serviços de rotina possam ser comprometidos) e, sempre que possível, deve ser executado fora do horário normal de expediente. Este procedimento somente deve ser realizado por pessoal especializado e autorizado pela COGEL/DITEC. O NTI dos órgãos deverá encaminhar tal solicitação, caso o serviço seja realizado no seu âmbito.

4.12.3. O download de softwares deve obedecer aos contratos estabelecidos com os fornecedores, quando aplicável.

4.12.4. Todo arquivo obtido em fontes externas à Administração Pública Municipal deve ser submetido à verificação de software antivírus antes de ser utilizado.

4.13 Competências do Núcleo de Tecnologia da Informação do Órgão ou Entidade:

4.13.1. prover os recursos necessários ao cumprimento desta Norma;

4.13.2. avaliar e homologar novos serviços de Internet antes de serem utilizados.

4.14 Documentos relacionados

- ABNT NBR ISO/IEC 27002:2022
- Norma 02 - Classificação da Informação. Norma 16 - Proteção Contra Código Malicioso.
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação.
- Norma 05 - Acesso e Utilização do Correio Eletrônico.
- Norma 06 - Gerenciamento de Incidentes de Segurança da Informação.
- Norma 11 - Intercâmbio de Informações.

4.15 Data de Revisão

20/11/2023.

5 Norma 04 - Acesso aos Recursos de Tecnologia da Informação

5.1 Objetivo

Estabelecer as diretrizes e responsabilidades para o acesso aos recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal.

5.2 Definições

Autenticação: processo de verificação que confirma se uma entidade ou um objeto é quem ou o que afirma ser, incluindo, em alguns exemplos, a confirmação da origem e da integridade das informações, tal como a verificação de uma assinatura digital ou da identidade de um utilizador ou de um computador.

Conta de Usuário: credencial de acesso à rede ou sistemas, de uso pessoal, intransferível e de responsabilidade de seu usuário designado.

Conta Genérica: credencial de acesso à rede que não identifica o usuário que a utiliza.

Credencial de Acesso: elemento utilizado para autenticar um usuário perante recursos de Tecnologia da Informação, tais como nome de usuário e senha, certificado digital, informação biométrica ou equivalentes.

Estação de Trabalho: todos os computadores e equipamentos correlatos da Administração Pública Municipal, inclusive dispositivos móveis.

Login/Logon: processo de autenticação com o objetivo de permitir o uso de um sistema computacional ou recursos de rede de forma segura.

Logoff: processo de encerramento do uso de um sistema computacional ou recursos de rede, removendo as credenciais de acesso.

Recursos de Tecnologia da Informação: estações de trabalho, servidores, redes, sistemas, serviços, banco de dados e dispositivos de interconexão.

Rede: estações de trabalho, servidores e outros dispositivos interligados que compartilham informações ou recursos da Administração Pública Municipal.

Smartcard: cartão de plástico com um microprocessador embutido, que utiliza criptografia para aplicar princípios da Segurança da Informação como: integridade, autenticidade e não repúdio.

Token: dispositivo, que juntamente com algo que o usuário conhece, como uma senha, vai autorizar o acesso a um sistema ou rede de computadores.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

5.3 Abrangência

Esta Norma se aplica a todos os usuários de informações ou recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal.

5.4 Concessão de Acesso

5.4.1. A licença para a utilização dos recursos de Tecnologia da Informação é uma concessão da Administração Pública Municipal aos usuários que necessitem deles para desempenhar suas funções.

5.4.2. A utilização poderá ser monitorada em tempo real e a licença poderá ser suspensa a qualquer momento por decisão do Gestor da área do usuário, da área de Tecnologia da Informação do órgão ou entidade, de acordo com os exclusivos critérios destes, visando evitar perda de produtividade e riscos de segurança.

5.4.3. O acesso à consulta ou utilização dos recursos de Tecnologia da Informação é permitido após a identificação do usuário, somente por meio de suas próprias credenciais de acesso.

5.4.4. As credenciais de acesso aos recursos de Tecnologia da Informação são pessoais, intransferíveis e de responsabilidade exclusiva do usuário, exceto para aqueles recursos que não suportarem a criação de credenciais individuais.

5.4.5. Toda solicitação, alteração, bloqueio e desbloqueio de acesso aos recursos de Tecnologia da Informação ou aos sistemas deve ser documentada.

5.4.6. O Gestor da área do usuário deve informar à área de Tecnologia da Informação do órgão ou entidade ou ao administrador do recurso de Tecnologia da Informação todos os direitos de acesso que o usuário deve possuir.

5.4.7. Todos os direitos de acesso aos recursos de Tecnologia da Informação devem ter prazo de vigência definido.

5.4.8. É expressamente proibida qualquer tentativa de acesso não autorizado aos recursos de Tecnologia da Informação.

5.4.9. A utilização de contas genéricas deve ser limitada ao estritamente necessário.

5.4.10. Os órgãos e entidades da Administração Pública Municipal que disponibilizem o acesso a recursos de Tecnologia da Informação ao cidadão devem desenvolver e comunicar regulamento específico para o bom uso desses recursos.

5.5 Conexão de Equipamentos

5.5.1. Somente dispositivos autorizados pela área de Tecnologia da Informação do órgão ou entidade poderão ter acesso aos recursos de rede da Administração Pública Municipal.

5.6 Gerenciamento de Senhas

5.6.1. A elaboração de senhas para acesso à rede ou aos sistemas deve ser realizada conforme procedimento estabelecido pela área de Tecnologia da Informação do órgão ou entidade, o qual deve prever troca periódica de senhas, senhas de difícil dedução e bloqueio automático da sessão por inatividade.

5.6.2. Todas as contas de usuário devem ter suas senhas alteradas no primeiro acesso a rede (logon na rede e nos sistemas de informação, para assegurar sua confidencialidade.

5.6.3. Os critérios para elaboração, manutenção e gerenciamento dos acessos devem levar em consideração a criticidade das informações e as necessidades dos processos de negócio envolvidos.

5.7 Análise Crítica

5.7.1. Os direitos de acesso dos usuários à rede e aos sistemas devem ser revisados periodicamente.

5.7.2. Os direitos de acesso dos usuários em afastamento definitivo da organização devem ser revogados.

5.7.3. Os direitos de acesso dos usuários em afastamento temporário devem ser suspensos no período da ausência.

5.7.4. Os direitos de acesso dos usuários em transferência de área devem ser revistos.

5.8 Competências

5.8.1 do Núcleo de Tecnologia da Informação do Órgão ou Entidade

5.8.1.1. administrar os acessos à rede e aos sistemas da Administração Pública Municipal;

5.8.1.2. elaborar procedimento de gerenciamento de senhas em consonância com a criticidade das informações e as necessidades dos processos de negócio envolvidos;

5.8.2 Das chefias dos setores

5.8.2.1. comunicar ao NTI todas as movimentações de pessoal que impliquem em concessão, mudança ou revogação de acessos de ambientes e sistemas corporativos;

5.8.2.2. comunicar ao NTI sempre que tomar ciência de direitos de acesso desnecessários à execução das atividades por parte de seus subordinados ou de terceiros.

5.8.3 Usuário

5.8.3.1. manter sigilo da senha de acesso à rede e aos sistemas, sendo de sua total e exclusiva responsabilidade qualquer operação realizada sob suas credenciais de acesso;

5.8.3.2. não compartilhar com terceiros sua credencial de acesso à rede ou aos sistemas;

5.8.3.3. informar ao Gestor do NTI quando forem identificados direitos de acesso desnecessários à execução das suas atividades profissionais;

5.8.3.4. bloquear sua estação de trabalho ou efetuar logoff da rede sempre que se ausentar de sua área de trabalho;

5.8.3.5. comunicar, imediatamente, ao NTI qualquer ocorrência de perda ou avaria de dispositivos adicionais de autenticação, tais como tokens, smartcards e outros.

5.9 Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2022
- Norma 03 - Uso da Internet.
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação.
- Norma 16 - Proteção Contra Código Malicioso.

5.10 Data de Revisão

18/10/2023

6 Norma 05 - Acesso e Utilização do Correio Eletrônico

6.1 Objetivo

Definir as diretrizes de acesso e utilização segura do Correio Eletrônico disponibilizado pela Administração Pública Municipal.

6.2 Definições

E-mail: forma reduzida para Electronic Mail - Correio Eletrônico.

Hiperlink: palavras ou endereços em destaque de uma página da Internet ou mensagem de Correio Eletrônico que, ao serem clicadas, efetuam o direcionamento para outra parte do texto da mensagem ou página da Internet.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

Webmail: é uma interface da Internet que permite consultar e enviar Correio Eletrônico (E-mail).

6.3 Abrangência

Esta Norma se aplica a todos os usuários que utilizam o serviço de Correio Eletrônico disponibilizado pela Administração Pública Municipal.

6.4 Diretrizes

6.4.1. O serviço de Correio Eletrônico corporativo é uma concessão da Administração Pública Municipal, sendo assim, seu uso é permitido somente para as atividades profissionais de seus usuários, não sendo permitido enviar ou arquivar mensagens não relacionadas às atividades profissionais, a exemplo de, mas não limitado a:

6.4.1.1. assuntos que provoquem assédio, constrangimento ou que prejudiquem a imagem da organização;

6.4.1.2. temas difamatórios, discriminatórios, material obsceno, ilegal ou antiético;

6.4.1.3. fotos, imagens, sons ou vídeos que não tenham relação com as atividades profissionais da organização.

6.4.2. As permissões de acesso a serviços de e-mail particulares, tais como webmail, podem ser estabelecidas e gerenciadas pelo NTI do órgão ou entidade e pelas áreas de negócio, em função dos interesses da Administração Pública;

6.4.3. O acesso ao Correio Eletrônico corporativo se dará, minimamente, pelo conjunto "Identificação do Usuário e Senha", que é pessoal e intransferível.

6.4.4. O endereço de e-mail disponibilizado ao usuário é de uso pessoal e intransferível e de responsabilidade dele. Portanto, é terminantemente proibido suprimir, modificar ou substituir a identidade do remetente de uma mensagem do Correio Eletrônico.

6.4.5. Havendo indícios de que mensagens veiculadas pelo correio eletrônico possam ocasionar quebra de segurança ou violação de quaisquer das vedações constantes deste ou de outro ato normativo, a área de Tecnologia da Informação do órgão ou entidade responsável pela administração do Serviço de Correio Eletrônico adotará, imediatamente, medidas para a apuração dessas irregularidades, utilizando-se dos meios e procedimentos legalmente previstos.

6.4.6. A disponibilização do Correio Eletrônico pode ser suspensa a qualquer momento por decisão do Gestor da área do usuário ou da área de Tecnologia da Informação do órgão ou entidade.

6.4.7. As concessões e revogações de acesso ao serviço de Correio Eletrônico devem ser autorizadas pelo Gestor da área do usuário por meio de uma solicitação de serviço à área de Tecnologia da Informação do órgão ou entidade.

6.4.8. Os anexos e/ou hiperlinks das mensagens de Correio Eletrônico poderão ser bloqueados quando oferecerem riscos à Segurança da Informação.

6.4.9. A abertura de mensagens de remetentes desconhecidos, externos à Administração Pública Municipal, deve ser avaliada, especialmente quando houver dúvidas quanto à natureza do seu conteúdo, como arquivos anexados não esperados ou hiperlinks para endereços externos não relacionados às atividades profissionais em curso.

6.4.10. A quantidade de destinatários deve ser limitada por mensagem, com o objetivo de coibir a prática de Spam. Cabe à área de Tecnologia da Informação do órgão ou entidade estabelecer tal limite, bem como acordar com as áreas de negócio as eventuais exceções, de acordo com os interesses da Administração Pública.

6.4.11. Todas as mensagens originárias de usuários da Administração Pública Municipal deverão conter a assinatura do remetente em formato padronizado estabelecido pela Secretaria de Gestão (SEMGE), além de um aviso legal, também padronizado, referenciando a confidencialidade da informação.

6.4.12. Limites de armazenamento das caixas de Correio Eletrônico devem ser estabelecidos pela área de Tecnologia da Informação do órgão ou entidade, considerando as necessidades dos processos de negócio que o serviço de Correio Eletrônico suporta, bem como limitações técnicas aplicáveis.

6.5 Competências

6.5.1 Área de Tecnologia da Informação do Órgão ou Entidade

- conceder, suspender e revogar os acessos ao serviço de Correio Eletrônico;
- administrar as funcionalidades e a segurança do serviço de Correio Eletrônico.

6.5.2 Chefia do setor do Usuário

- comunicar à área de Tecnologia da Informação do órgão ou entidade todas as movimentações de pessoal que impliquem em concessão, mudança ou revogação de acessos.

6.5.3 Usuário

- responder pelo uso adequado dos serviços e recursos de Correio Eletrônico a ele disponibilizados, nas suas mais diversas formas de acesso, inclusive por meio de dispositivos móveis, em consonância com esta Norma.

6.6 Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2022
- Norma 03 - Uso da Internet.
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação.
- Norma 16 - Proteção Contra Código Malicioso.

6.7 Data de Revisão

18/10/2023

7 Norma 06 - Gerenciamento de Incidentes de Segurança da Informação

7.1 Objetivo

Normatizar o registro e o tratamento de incidentes de Segurança da Informação no âmbito da Administração Pública Municipal.

7.2 Definições

Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio.

Log: arquivo que contém informações sobre eventos de qualquer natureza em um sistema computacional, análise forense para a elucidação de incidentes de segurança, auditoria de processos, cumprimento de exigências legais para a manutenção de registro do histórico de acessos ou eventos e para a resolução de problemas (debugging).

Usuário: qualquer colaborador seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza os recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

7.3 Abrangência

Esta Norma se aplica a todos os usuários de informações ou recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal.

7.4 Diretrizes

7.4.1. Todo usuário deve registrar incidentes de Segurança da Informação, conforme orientações descritas em procedimento específico.

7.4.2. A área de Tecnologia da Informação do órgão ou entidade deve registrar um incidente de Segurança da Informação para toda falha de segurança identificada nos recursos de Tecnologia da Informação da Administração Pública Municipal.

7.4.3. As informações referentes aos responsáveis pelo registro de incidentes de Segurança da Informação são sigilosas, entretanto esta identificação é obrigatória.

7.4.4. A área de Tecnologia da Informação do órgão ou entidade deve garantir que planos de ação sejam elaborados para tratamento de incidentes, e monitorar sua implementação.

7.4.5. É vedado ao usuário intervir no tratamento dos incidentes sem a devida autorização ou qualificação.

7.5 Competências

7.5.1 Área de Tecnologia da Informação do Órgão ou Entidade:

7.5.1.1. identificar e documentar incidentes de Segurança da Informação por meio de análise dos logs dos recursos de Tecnologia da Informação;

7.5.1.2. reportar todos os incidentes de Segurança da Informação à COGEL/DITEC, de forma regular;

7.5.1.3. elaborar Planos de Recuperação de Desastres (PRD) para os processos críticos;

7.5.1.4. executar procedimentos e ações corretivas quando necessário;

7.5.1.5. informar ao usuário as ações tomadas em relação aos incidentes registrados, quando aplicável.

7.5.2 Gestor da Área do Usuário

7.5.2.1. apoiar a área de Tecnologia da Informação do órgão ou entidade na solução dos incidentes de Segurança da Informação;

7.5.2.2. apoiar na execução das ações corretivas/preventivas estabelecidas para o tratamento dos incidentes;

7.5.2.3. apoiar a área de Tecnologia da Informação do órgão ou entidade, na elaboração e implementação dos planos de contingência para diferentes tipos de incidentes de segurança, visando reduzir os impactos, restabelecendo os processos de negócio afetados, o mais rápido possível.

7.5.3 Usuário

7.5.3.1. registrar incidentes de Segurança da Informação.

7.6 Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2022
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação.

7.7 Data de Revisão

18/10/2023

8 Norma 07 - Gerenciamento da Auditoria de Segurança da Informação

8.1 Objetivo

Definir as diretrizes do processo de Auditoria de Segurança da Informação, no âmbito da Administração Pública Municipal.

8.2 Definições

Alta Administração: dirigente máximo dos órgãos e entidades da Administração Pública Municipal, chefes de gabinete, superintendentes e diretores. A Alta Administração dos órgãos e entidades também pode ser proprietária, custodiante ou usuária da informação.

Custodiante da Informação: aquele que armazena, processa, veicula e trata a informação, mediante orientação dada pela classificação e assume, em conjunto com o proprietário da informação, a responsabilidade pela proteção desta.

Proprietário da Informação: aquele que gera ou adquire a informação.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

8.3 Abrangência

Esta Norma se aplica a todos os processos de negócio da Administração Pública Municipal.

8.4 Diretrizes

8.4.1. Toda Auditoria de Segurança da Informação deve estar autorizada de acordo com a legislação vigente.

8.4.2. A necessidade de Auditoria de Segurança da Informação deve ser verificada regularmente, produzindo um relatório de diretrizes de auditoria. Essa verificação deve contemplar, entre outros:

8.4.2.1. análise dos documentos que compõem a Política de Segurança da Informação;

8.4.2.2. resultados de auditorias anteriores;

8.4.2.3. indicadores de Segurança da Informação;

8.4.2.4. análise dos incidentes de Segurança da Informação registrados;

8.4.2.5. informações relativas a análises de risco.

8.4.3. Requisitos e atividades de Auditoria de Segurança da Informação devem ser planejados para minimizar o risco de interrupção dos processos de negócio envolvidos, devendo o planejamento contemplar, dentre outros:

8.4.3.1. áreas, usuários, processos e sistemas que serão auditados;

8.4.3.2. controles de Segurança da Informação que serão auditados;

8.4.3.3. estratégia de comunicação com todos os envolvidos;

8.4.3.4. identificação dos auditores;

8.4.3.5. independência dos auditores em relação às atividades auditadas;

8.4.3.6. cronograma de execução da auditoria.

8.4.4. Os auditores devem ter acesso apenas à leitura de software e dados, só sendo permitido outros acessos por meio de cópias isoladas e estes devem ser apagados ao final da auditoria, ou dada a devida proteção quando houver a obrigação ou necessidade de armazenar tais cópias.

8.4.5. Quando o acesso a dados sensíveis for indispensável para os objetivos da auditoria, mecanismos adicionais devem ser implementados para garantia de sua confidencialidade.

8.4.6. Mecanismos que garantam o registro de todas as atividades da auditoria devem ser implementados, de forma a produzir uma trilha de referência.

8.4.7. O acesso às ferramentas de auditoria deve ser restrito e controlado, visando prevenir uso não autorizado.

8.4.8. O processo de auditoria deve produzir relatórios contendo, dentre outros, os dados da área, do usuário, o processo ou sistema auditado, os controles verificados, evidências para conformidades e justificativas para não conformidades.

8.4.9. Os dados destes relatórios devem alimentar o processo de Gestão de Indicadores de Segurança da Informação.

8.4.10. Um plano com ações preventivas e corretivas deve ser elaborado com base no relatório gerado pelo processo de auditoria.

8.4.11. O resultado de auditorias de Segurança da Informação deve ser caracterizado como informação sigilosa quando esse puder comprometer a segurança dos processos de negócio do órgão ou entidade a que se refere.

8.4.12. Uma análise crítica dos resultados da auditoria deve ser conduzida, com o objetivo de determinar ações de melhoria para possíveis ajustes na Política de Segurança da Informação.

8.5 Competências

8.5.1 Auditor

8.5.1.1. planejar a Auditoria de Segurança da Informação em conjunto com a área de Tecnologia da Informação do órgão ou entidade;

8.5.1.2. conduzir auditorias, elaborar relatórios com os resultados e apresentar recomendações de ações preventivas e corretivas.

8.5.2 Áreas de Negócio do Órgão ou Entidade

8.5.2.1. elaborar e implementar planos de ação para prevenção e correção de não conformidades observadas durante o processo de auditoria.

8.5.2.2. Área de Tecnologia da Informação do Órgão ou Entidade

8.5.2.3. identificar necessidades de Auditoria da Segurança da Informação;

8.5.2.4. prover os recursos necessários para a execução da auditoria;

8.5.2.5. garantir a segurança dos dados gerados pelo processo de auditoria;

8.5.2.6. apoiar a implementação dos planos de ação relativos à auditoria, gerados pelas áreas de negócio;

8.5.2.7. conduzir análises críticas com vistas ao aprimoramento da Política de Segurança da Informação do órgão ou entidade da Administração Pública Municipal.

8.6 Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2022

8.7 Data de Revisão

18/10/2023

9 Norma 08 - Gestão de Continuidade de Negócios

9.1 Objetivo

Estabelecer, no âmbito da Administração Pública Municipal, as regras e os princípios que regulamentam a Gestão da Continuidade do Negócio (GCN), que são: manter o negócio em funcionamento, definir o papel de cada elemento que administrará a situação da GCN e conscientizar todos os usuários sobre suas responsabilidades no processo.

9.2 Definições

Continuidade do Negócio: capacidade estratégica e tática do órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios para conseguir continuar suas operações em um nível aceitável e previamente definido.

Gestão de Continuidade de Negócios: processo de gestão que identifica ameaças em potencial e os possíveis impactos às operações de negócio caso essas ameaças se concretizem. Este processo fornece um framework para que se construa uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar a reputação e a marca do órgão ou entidade e suas atividades de valor agregado.

Partes Interessadas: aqueles que possuem um interesse permanente nos resultados de uma organização.

Plano de Continuidade de Negócios (PCN): conjunto de procedimentos e planos que visa garantir a continuidade das operações normais da organização, mesmo após ocorrência de um desastre ou indisponibilidade de recursos que sustentam os processos de negócio.

Resiliência Organizacional: capacidade do órgão ou entidade de reagir a um incidente de Segurança da Informação que provoque a interrupção das operações críticas, a tempo de reduzir ou eliminar os danos desta interrupção, incluindo a capacidade estratégica e tática para planejar e responder a incidentes e interrupções do negócio com a finalidade de continuar as operações do negócio a um nível pré-definido e aceitável.

Sistema de Gestão de Continuidade de Negócios (SGCN): parte do sistema global de gestão que estabelece, implementa, opera, monitora, analisa criticamente, mantém e melhora a continuidade de negócios.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

9.3 Abrangência

Esta Norma se aplica a todos os usuários e processos da Administração Pública Municipal, bem como, aos sistemas informatizados e meios convencionais de processamento, comunicação e armazenamento de informações.

9.4 Diretrizes

9.4.1. A Gestão da Continuidade de Negócio (GCN) na Administração Pública Municipal deve sistematizar o entendimento integral de todos os aspectos e fenômenos relacionados à Continuidade do Negócio, incluindo:

9.4.1.1. identificação das ameaças potenciais e os respectivos impactos nas operações do negócio do órgão ou entidade;

9.4.1.2. definição da estratégia de recuperação a ser utilizada caso ocorra um incidente;

9.4.1.3. gerenciamento de incidente adverso que interrompa um processo ou atividade crítica;

9.4.1.4. planejamento da continuidade e da recuperação das operações e sistemas após uma interrupção;

9.4.1.5. estabelecimento de procedimentos de retorno à normalidade, quando aplicável;

9.4.1.6. o desenvolvimento de novos produtos e serviços críticos dos órgãos e entidades, assim como mudanças nos existentes, devem ser seguidos por atualizações no PCN para que suas estratégias e ações continuem válidas;

9.4.1.7. estabelecer um programa efetivo para planejamento, resposta a incidentes e a interrupções nos processos de negócio;

9.4.1.8. prover a continuidade das operações do negócio em um nível aceitável;

9.4.1.9. aumentar o poder de recuperação da organização contra o rompimento ou interrupção de sua habilidade de fornecer seus produtos e serviços;

9.4.1.10. orientar ações de prevenção e mitigação dos riscos operacionais;

9.4.1.11. prover a organização de uma metodologia para a elaboração do PCN que possibilite o restabelecimento da sua habilidade de fornecer seus produtos e serviços críticos;

9.4.1.12. desenvolver e implementar um Sistema de Gestão de Continuidade de Negócios para os órgãos ou entidades, que deve ser aceito e seguido inclusive pelas empresas prestadoras de serviço;

9.4.1.13. estabelecer um programa de treinamento e conscientização dos usuários.

9.5 Competências

9.5.1 Alta Administração do Órgão ou Entidade

– prover apoio estratégico à Gestão da Continuidade de Negócio.

9.5.2 Gestores das Áreas de Negócio do Órgão ou Entidade

– viabilizar, atualizar, manter e implementar os Planos de Continuidade de Negócios.

9.5.3 Usuários

– conhecer os planos existentes e as situações em que serão utilizados, além dos procedimentos em que sua participação esteja prevista.

9.6 Documentos Relacionados

– ABNT NBR ISO/IEC 27001:2022
– ABNT NBR ISO/IEC 27002:2022
– ISO/IEC Guide 73:2009 - Gestão de riscos - Vocabulário.
– Sistemas de Gestão da Continuidade do Negócio – BS/ISO 22313:2012
– Normas de Controle de TI, Cobit – Control Objectives for Information and related Technology.
– ABNT NBR15999-1:2007 - Versão corrigida 2008 - Gestão de Continuidade de Negócios - Parte 1: Código de prática.
– ABNT NBR ISO/IEC 22301:2013 – Segurança da Sociedade – Sistema de Gestão de Continuidade de Negócios - Requisitos.
– ABNT NBR ISO/IEC 27005:2011 - Tecnologia da Informação - Técnicas de segurança - Gestão de Riscos de Segurança da Informação.

9.7 Data de Revisão

18/10/2023.

10 Norma 09 - Gestão de Riscos

10.1 Objetivo

Estabelecer as diretrizes do processo de Gestão de Riscos no âmbito da Segurança da Informação para a Administração Pública Municipal.

10.2 Definições

Alta Administração: dirigente máximo dos órgãos e entidades da Administração Pública Municipal, chefes de gabinete, superintendentes e diretores. A Alta Administração dos órgãos e entidades também pode ser proprietária, custodiante ou usuária da informação.

Análise de Riscos: processo de compreender a natureza do risco e determinar o seu nível.

Avaliação de Riscos: processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis.

Controle: qualquer processo, política, dispositivo, prática ou outras ações que modifiquem o risco, podendo ser de natureza administrativa, técnica, de gestão ou legal.

Risco: combinação de consequências de um evento e a probabilidade de ocorrência associada.

Risco Residual: risco remanescente após o seu tratamento.

Tratamento de Riscos: processo de seleção e implementação de medidas para modificar riscos.

10.3 Abrangência

Esta Norma se aplica a todos os processos críticos de negócio da Administração Pública Municipal.

10.4 Diretrizes

10.4.1. Deve ser estabelecida uma metodologia para Gestão de Riscos, contemplando a definição do contexto, análise e avaliação, tratamento, aceitação e comunicação de riscos.

10.4.2. A Gestão de Riscos deve ser um processo contínuo, através de constante monitoramento e análise crítica dos riscos para os processos de negócio.

10.4.3. Deve ser definido um período para o ciclo de análises de risco.

10.4.4. Análises críticas devem ser conduzidas com o objetivo de melhoria do próprio processo de gerenciamento de riscos.

10.5 Definição do Contexto de Riscos

10.5.1. Deve ser definido um contexto para toda análise de riscos, contemplando, entre outros:

10.5.1.1. objetivos estratégicos da Administração Pública Municipal;

10.5.1.2. formalização do escopo da análise de riscos;

10.5.1.3. avaliação de requisitos de Segurança da Informação;

10.5.1.4. incidentes de Segurança da Informação;

10.5.1.5. política de Segurança da Informação;

10.5.1.6. resultados de análises de riscos anteriores;

10.5.1.7. monitoração do ambiente externo, identificando ameaças, riscos e vulnerabilidades.

10.6 Análise de Riscos

10.6.1. Uma análise dos relacionamentos existentes entre os processos de negócio, seus sistemas e serviços, e, respectivos ativos, deve ser conduzida em sintonia com o contexto definido, para estabelecer as prioridades da análise de riscos.

10.6.2. As análises de riscos devem ser executadas como projetos. Cada projeto deve ter a ciência da Alta Administração do órgão ou entidade e um responsável definido.

10.6.3. As análises de riscos devem ser planejadas, contemplando uma avaliação do escopo da análise, definição de cronograma, estratégia de comunicação e estimativa de custos, quando aplicável.

10.6.4. As análises de riscos devem gerar relatórios operacionais e executivos com o objetivo de auxiliar a fase de avaliação de riscos.

10.7 Avaliação de Riscos

10.7.1. Processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis.

10.7.2. Com base nos critérios de risco estabelecidos, os riscos aceitáveis devem ser aceitos formalmente pela Alta Administração e os riscos não aceitáveis devem ser tratados.

10.8 Tratamento e Comunicação de Riscos

10.8.1. O tratamento de riscos deve ser planejado, através da definição:

10.8.1.1. dos controles a serem implementados e de seus responsáveis;

10.8.1.2. da identificação de premissas e restrições, quando aplicáveis;

10.8.1.3. da definição de um cronograma de implementação.

10.8.2. Antes da implementação de qualquer controle, deverá ser feita uma análise de impacto no ambiente que sofrerá a mudança.

10.8.3. Todos os controles não implementados devem ser formalmente documentados e justificados.

10.8.4. Ao final da fase de tratamento, relatórios devem ser elaborados contemplando:

10.8.4.1. o escopo das implementações;

10.8.4.2. a equipe envolvida no processo;

10.8.4.3. os controles implementados;

10.8.4.4. os índices de risco e conformidade pré e pós implementações;

10.8.4.5. os riscos residuais.

10.8.5. O resultado das Análises e Avaliações de Risco de Segurança da Informação deve ser classificado como informação sigilosa, quando esse puder comprometer a segurança dos processos de negócio do órgão ou entidade a que se refere.

10.9 Competências

10.9.1 Alta Administração do Órgão ou Entidade

10.9.1.1. autorizar e viabilizar o processo de gestão de riscos;

10.9.1.2. estabelecer e formalizar os critérios de aceitação dos riscos e os objetivos dos índices de risco e de conformidade.

10.9.2 Áreas de Negócio do Órgão ou Entidade

10.9.2.1. em conjunto com a área de Tecnologia da Informação, analisar os resultados provenientes das análises de riscos executadas nos ativos sob sua responsabilidade, definindo planos de ação para aplicação dos controles recomendados, quando aplicável;

10.9.2.2. aceitar ou tratar os riscos conforme os critérios estabelecidos pela Alta Administração do órgão ou entidade.

10.9.3 Área de Tecnologia da Informação do Órgão ou Entidade

10.9.3.1. viabilizar a implementação dos controles sob sua competência;

10.9.3.2. estabelecer o contexto de riscos em conjunto com as áreas envolvidas;

10.9.3.3. executar periodicamente os processos de análise, avaliação, comunicação e tratamento de riscos.

10.10 Documentos Relacionados

- ABNT NBR ISO 31000:2009 - Gestão de Riscos - Princípios e diretrizes.
- ABNT NBR ISO/IEC 27005:2011– Tecnologia da Informação – Técnicas de Segurança - Gestão de Riscos de Segurança da Informação.

10.11 Data de Revisão

18/10/2023

11 Norma 10 - Contabilização de Ativos de Tecnologia da Informação

11.1 Objetivo

Definir as diretrizes para a contabilização adequada dos Ativos de Tecnologia da Informação no âmbito da Administração Pública Municipal.

11.2 Definições

Ativos de Tecnologia da Informação: estações de trabalho, servidores, softwares, mídias e quaisquer equipamentos eletrônicos relacionados à Tecnologia da Informação, bem como processos, pessoas e ambientes.

Estação de Trabalho: todos os computadores e equipamentos correlatos da Administração Pública Municipal, inclusive dispositivos móveis.

Freeware: programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso.

Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio.

Mídias Removíveis/Reutilizáveis: incluem fitas, discos, memórias flash, discos removíveis, CD, DVD, mídia impressa, entre outros.

Shareware: programa disponível publicamente para avaliação e uso experimental, mas, cujo uso em regime pressupõe que o usuário pagará uma licença ao autor. Shareware é distinto de freeware, no sentido de que um software shareware é comercial, embora em termos e preços diferenciados em relação a um produto comercial convencional.

Software Livre: denominação dada a determinado software cujo código-fonte é de domínio público e, em geral, gratuito.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

11.3 Abrangência

Esta Norma se aplica a todos os usuários dos Ativos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal.

11.4 Diretrizes

11.4.1. As informações e os Ativos de Tecnologia da Informação de propriedade da Administração Pública Municipal devem ser utilizados exclusivamente para os seus interesses, podendo ser monitorados a qualquer tempo.

11.4.2. Os Ativos de Tecnologia da Informação devem ser inventariados e identificados de forma única.

11.4.3. Os Ativos de Tecnologia da Informação devem ser classificados em função de sua relevância para o processo de negócio a que se destinam. Esta relevância deve ser considerada em eventuais análises de riscos

11.4.4. Os Ativos de Tecnologia da Informação devem ser, sempre que possível, relacionados a um usuário, responsável por sua utilização.

11.4.5. A entrada e a saída de Ativos de Tecnologia da Informação das dependências dos órgãos e entidades da Administração Pública Municipal devem ser acompanhadas pelos devidos documentos de movimentação.

11.4.6. O padrão de configuração (hardware e software) dos Ativos de Tecnologia da Informação é definido pela área de Tecnologia da Informação dos órgãos e entidades e não deve ser modificado sem sua autorização.

11.4.7. Os itens que compõem conjuntos de ativos não podem ser modificados sem a autorização da área de Tecnologia da Informação dos órgãos e entidades.

11.4.8. Somente softwares licenciados e homologados devem ser utilizados.

11.4.9. Os inventários (hardware e software) devem ser atualizados apropriadamente sempre que Ativos de Tecnologia da Informação sofrerem mudanças.

11.4.10. As mídias contendo as cópias de segurança devem ser catalogadas e armazenadas por tempo compatível com as necessidades dos processos de negócio.

11.4.11. A utilização de software que não seja de propriedade da Administração Pública Municipal ou licenciado para ela, pode, além de configurar crime de pirataria conforme Lei Nº 9.609, de 19 de fevereiro de 1998, interferir na contabilização dos ativos.

11.5 Competências

11.5.1 Área de Tecnologia da Informação do Órgão ou Entidade

11.5.1.1. contabilizar os Ativos de Tecnologia da Informação de forma a garantir sua conformidade com esta Norma.

11.5.2 Usuário

11.5.2.1. utilizar os Ativos de Tecnologia da Informação em conformidade com esta Norma

11.5.2.2. notificar, através de abertura de incidente de Segurança da Informação, sempre que identificar dano, roubo, perda ou modificações indevidas em um Ativo de Tecnologia da Informação.

11.6 Documentos Relacionados

- Norma 04 - Acesso aos Recursos de Tecnologia da Informação.
- Norma 06 - Gerenciamento de Incidentes de Segurança da Informação.

11.7 Data de Revisão

18/10/2023

12 Norma 11 - Intercâmbio de Informações

12.1 Objetivo

Definir as diretrizes de segurança na troca de informações e softwares internamente, entre os órgãos e entidades da Administração Pública Municipal e/ou com quaisquer entidades externas.

12.2 Definições

Criptografia: técnica utilizada para tornar a informação original ilegível, permitindo que somente o destinatário (detentor da chave de criptografia) a decifre.

Informação Sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Mídias Removíveis/Reutilizáveis: incluem fitas, discos, memórias flash, discos removíveis, CD, DVD, mídia impressa, entre outros.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

Virtual Private Network (VPN): rede virtual privada com uso de criptografia para garantir a confidencialidade das informações trafegadas em uma rede pública.

12.3 Abrangência

Esta Norma se aplica a todos os usuários de informações ou sistemas de informação de propriedade da Administração Pública Municipal.

12.4 Diretrizes

12.4.1. A troca de informações entre os usuários deve ser suportada por acordos formalizados e documentados, contendo, quando aplicável, cláusulas de preservação da privacidade de dados pessoais, direitos autorais, preservação de bens patrimoniais, sigilo e não divulgação.

12.4.2. Salvo nos casos previstos em lei, todo usuário deve assinar um termo de sigilo e confidencialidade com a Prefeitura Municipal de Salvador.

12.4.3. As informações classificadas como sigilosas gravadas em mídia removível devem utilizar solução de criptografia.

12.4.4. Toda informação sigilosa deve receber o tratamento adequado conforme descrito na Norma 02 - Classificação da Informação.

12.4.5. Procedimentos de recepção de fac-símiles, impressão de documentos, abertura de correio e distribuição de correspondência devem ser estabelecidos de forma a prevenir o acesso não autorizado à informação. Ações de conscientização dos usuários devem incluir a observância das necessidades de segurança ao se efetuar conversações, inclusive as telefônicas, sobre assuntos restritos e confidenciais em locais públicos, em escritórios abertos ou mesmo em reuniões realizadas em sala sem a devida adoção dos requisitos de segurança.

12.4.6. Mecanismos devem ser implementados para proteger as informações associadas aos sistemas de informação dos negócios, entre outros:

12.4.6.1. proteção contra interceptação e gravação de chamadas telefônicas ou de teleconferências, garantindo a confidencialidade das chamadas;

12.4.6.2. o acesso à rede corporativa ou a Intranet, por meio da Internet, deve utilizar solução de criptografia, a exemplo de VPN (Virtual Private Network);

12.4.6.3. procedimento de retenção de cópias de segurança das informações mantidas nos sistemas, bem como sua recuperação e contingência;

12.4.6.4. restrição de acesso a informações de trabalho compatível às atividades do usuário através do gerenciamento de perfis de acesso;

12.4.6.5. proteção contra código malicioso, conforme Norma de Proteção Contra Código Malicioso;

12.4.6.6. procedimentos para o uso de comunicação sem fio, levando em conta os riscos particulares envolvidos;

12.4.6.7. as mensagens confidenciais, enviadas pelo Correio Eletrônico, devem utilizar solução de criptografia.

12.5 Mídias em Trânsito

12.5.1. Devem ser adotados transporte e serviço de mensageiro confiável e preferencialmente estabelecer um contrato de sigilo e confidencialidade com esse serviço.

12.5.2. As embalagens de mídias removíveis devem ser suficientes para proteger os conteúdos contra danos físicos.

12.5.3. Mecanismos de proteção contra danos físicos durante o transporte das mídias removíveis devem ser adotados, considerando as recomendações do fabricante das mídias.

12.5.4. A entrega dos documentos e das mídias removíveis, contendo informações sigilosas, deve ser registrada em recibo ou sistema eletrônico específico.

12.6 Competências

12.6.1 Área de Tecnologia da Informação do Órgão ou Entidade

12.6.1.1. prover recursos para garantir a troca adequada de software, de informações armazenadas e transmitidas por meio eletrônico.

12.6.2 Usuário

12.6.2.1. cumprir as diretrizes desta norma.

12.7 Documentos Relacionados

- Norma 02 - Classificação da Informação.
- Norma 05 - Acesso e Utilização do Correio Eletrônico.
- Norma 16 - Proteção Contra Código Malicioso.

12.8 Data de Revisão

18/10/2023

13 Norma 12 - Segurança Física

13.1 Objetivo

Estabelecer diretrizes para prevenir o acesso físico não autorizado, a fim de evitar danos e interferência às informações, ativos e instalações físicas da Administração Pública Municipal.

13.2 Definições

Área Protegida: corresponde às dependências dos órgãos e entidades, onde escritórios, salas e instalações de processamento de informações são utilizados pela Administração Pública Municipal.

Área Pública: corresponde ao perímetro externo às dependências dos órgãos e entidades, tais como ruas, avenidas e áreas circunvizinhas e instalações prediais, quando as dependências do órgão ou entidade estão em salas ou andares de prédios comerciais.

Área Segura: incluem-se nesta classificação especial as áreas protegidas que contenham informações, dispositivos ou serviços imprescindíveis aos negócios, tais como sala de servidores, sala de operação, cofre, salas e armários com informações sensíveis associadas a interesses relevantes dos órgãos e entidades e locais com equipamentos e infraestrutura de conectividade (switches, roteadores, dispositivos de armazenamento, quadro de telefonia, quadro de cabeamento, entre outros).

13.3 Abrangência

Esta Norma se aplica a todas as dependências e usuários da Administração Pública Municipal.

13.4 Diretrizes

13.4.1. Perímetros de Segurança. As regras de controle de acesso físico não se aplicam às áreas públicas.

13.5 Em Áreas Protegidas

13.5.2. devem ser localizados de forma a evitar o acesso do público, com indicações mínimas do seu propósito e sem sinais óbvios da presença de atividades de processamento de informação;

13.5.3. convém que as paredes externas possuam construção sólida. As portas externas devem ser protegidas de forma apropriada, com mecanismos de controle, travas etc., contra acessos não autorizados; uma área de recepção ou outro meio de controle de acesso físico deve ser usado, devendo o acesso ser restrito apenas ao pessoal autorizado;

13.5.4. barreiras físicas devem, se necessário, ser estendidas da laje do piso até a laje superior para prevenir acessos não autorizados ou contaminação ambiental como as causadas por fogo e inundações;

13.5.5. todas as portas de incêndio devem possuir dispositivo para fechamento automático;

13.5.6. devem ser afixados avisos (normalmente nas entradas, saídas e corredores de acesso), facilmente visíveis, informando sobre o controle de acesso para as pessoas e alertando sobre as restrições ao acesso público, de tal forma que desestimule as invasões.

13.6 Em Áreas Seguras

13.6.1. barreiras e perímetros adicionais para controlar o acesso físico podem ser necessários em áreas com diferentes requisitos de segurança dentro de um mesmo perímetro de segurança;

13.6.2. devem ser afixados avisos, normalmente na respectiva porta, facilmente visíveis, alertando sobre as restrições ao acesso às áreas seguras, indicando que somente pessoal autorizado tem acesso, de tal forma que desestimule as invasões.

13.7 Controles de Entrada Física

13.7.1. Procedimentos de controle de acesso físico devem ser implementados de forma a restringir o acesso às áreas protegidas e seguras. Os procedimentos de controle de acesso devem, quando necessário, contemplar, entre outros:

13.7.1.1. a utilização de dispositivos de identificação pessoal;

13.7.1.2. monitoração de acessos;

13.7.1.3. restrições de horários de acesso e permanência;

13.7.1.4. controle de acesso de terceiros;

13.7.1.5. movimentação de ativos.

13.7.2. O pessoal autorizado deve ter acesso físico somente aos ativos imprescindíveis para a realização dos seus trabalhos.

13.7.3. O acesso de visitantes deve se dar somente após identificação individual e autorização de entrada por parte da pessoa e/ou setor que será visitado.

13.8 Segurança em Escritórios, Salas e Instalações de Processamento

13.8.1. A escolha da localização, os projetos de engenharia e arquitetura das instalações devem levar em consideração as possibilidades de danos causados por fogo, inundações, explosões, manifestações civis e outras formas de desastres naturais ou causados pelo homem. Também devem ser levados em consideração as regulamentações e padrões de segurança e saúde, bem como serem tratadas quaisquer ameaças originadas em propriedades vizinhas.

13.8.2. Portas e janelas devem ser mantidas fechadas quando não utilizadas e devem ser instaladas proteções extras, principalmente quando essas portas e janelas se localizarem em andar térreo.

13.8.3. Sistemas de detecção de intrusos, tais como alarmes e sistemas de vídeo vigilância, devem ser instalados e testados regularmente, de forma a cobrir todas as portas e janelas acessíveis.

13.8.4. Equipamentos de contingência e meios magnéticos de reserva devem ser guardados a uma distância segura para evitar danos que podem se originar de um desastre na área protegida.

13.8.5. As portas de entrada devem permanecer trancadas nos períodos de inatividade.

13.8.6. Uma “política de mesa limpa” deve ser implementada, visando eliminar riscos de acesso não autorizado a informações em mídias não magnéticas, tais como documentos sensíveis deixados em impressoras ou mesas de trabalho.

13.9 Trabalho em Áreas Seguras

13.9.1. A existência das informações ou das atividades dentro de áreas seguras deve ser de conhecimento restrito a pessoal autorizado e apenas quando necessárias.

13.9.2. Áreas seguras devem estar fechadas e trancadas adequadamente de forma a impedir acessos não autorizados. Quando desocupadas, devem ser mantidas fisicamente fechadas e verificadas periodicamente.

13.9.3. Somente pessoas imprescindíveis à realização dos trabalhos rotineiros ou de manutenção devem ter acesso às áreas seguras, mediante autorização.

13.9.4. Deve-se evitar trabalho sem monitoramento nas áreas seguras para prevenir oportunidades de atividades maliciosas, devendo o pessoal de serviços de suporte terceirizado ter acesso controlado a estas áreas.

13.9.5. Materiais combustíveis ou perigosos devem ser guardados de forma adequada a uma distância apropriada de uma área segura.

13.9.6. Suprimentos volumosos, tais como material de escritório, não devem ser guardados em áreas seguras, a menos que sejam imprescindíveis.

13.9.7. Qualquer equipamento de gravação, fotográfico, vídeo ou som somente deve ser utilizado com autorização.

13.10 Instalação e Proteção dos Equipamentos

13.10.1. Os Ativos de Tecnologia da Informação devem ser posicionados fisicamente e protegidos, a fim de se reduzir o risco decorrente de ameaças potenciais e oportunidades de acesso não autorizado.

13.10.2. O consumo de alimentos, bebidas e fumo deve acontecer apenas nas instalações definidas para esse fim.

13.10.3. Os Ativos de Tecnologia da Informação críticos devem ser protegidos por equipamentos contra falhas de energia e outras anomalias na alimentação elétrica.

13.10.4. As áreas consideradas pela Administração Pública Municipal como sendo de alto risco devem possuir planos de continuidade operacional que estabeleçam as atividades necessárias para contingência e restauração dos Ativos de Tecnologia da Informação, de forma a garantir a disponibilidade dos serviços, mesmo em momentos de crise.

13.10.5. Normas Técnicas Brasileiras devem ser seguidas no que concerne ao cabeamento de redes, telecomunicações e instalações elétricas.

13.10.6. O cabeamento de dados e as instalações elétricas devem ser protegidos contra interceptação ou dano.

13.10.7. Os pontos de rede de dados devem ser controlados, devendo-se documentar todos os pontos existentes e evitar a existência de pontos ativos sem utilização.

13.11 Competências

13.11.1 Área de Tecnologia da Informação do Órgão ou Entidade

13.11.1.1. garantir que os Ativos de Tecnologia da Informação estejam fisicamente protegidos contra ameaças à sua segurança, conforme as diretrizes desta Norma;

13.11.1.2. realizar auditorias periódicas visando o cumprimento das diretrizes desta Norma;

13.11.1.3. tratar os incidentes de segurança abertos em função de não conformidades observadas.

13.11.2 Usuário

13.11.2.1. observar e cumprir todas as diretrizes desta Norma;

13.11.2.2. reportar quaisquer não conformidades através de abertura de incidente de segurança.

13.12 Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2022
- Norma 06 - Gerenciamento de Incidentes de Segurança da Informação.

13.13 Data de Revisão

18/10/2023

14 Norma 13 - Segurança em Terceirização e Prestação de Serviços

14.1 Objetivo

Estabelecer diretrizes para implementar e manter o nível apropriado de Segurança da Informação e de entrega de serviços nos acordos firmados entre a Prefeitura Municipal de Salvador (PMS) e terceiros.

14.2 Definições

Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio.

Parceiro: qualquer entidade pública ou privada, organizações não governamentais ou instituições sem fins lucrativos com a qual se estabeleça uma relação de cooperação mútua.

Terceiro: qualquer parceiro, fornecedor ou prestador de serviço que acesse informações ou utilize recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal.

14.3 Abrangência

Esta Norma se aplica a todos os acordos celebrados entre a Prefeitura de Salvador e terceiros.

14.4 Diretrizes

14.4.1. Contratos firmados entre a Prefeitura de Salvador e prestadores de serviço devem incluir acordos que definam os níveis de entrega de serviços, contemplando, entre outros:

14.4.1.1. definição explícita das responsabilidades e direitos legais da Prefeitura de Salvador, da Prestadora de Serviços e dos profissionais envolvidos;

14.4.1.2. definição explícita dos direitos de propriedade dos produtos gerados;

14.4.1.3. aceite obrigatório de toda a Política de Segurança da Informação do contratante;

14.4.1.4. acordos de confidencialidade entre ambas as partes;

14.4.1.5. acordos de confidencialidade entre o terceiro e seus funcionários e subcontratados;

14.4.1.6. limitação do acesso apenas aos ativos e informações necessários à execução de suas atividades;

14.4.1.7. cláusulas contratuais que garantam a continuidade operacional durante os períodos de transição;

14.4.1.8. nível de capacidade técnica, logística e administrativa necessária do terceiro para prestar os serviços contratados;

14.4.1.9. planos para garantir os níveis de continuidade de serviços acordados após falhas severas nos serviços ou desastres;

14.4.1.10. acordos de nível de serviço (SLA), com indicadores adequados à natureza do contrato;

14.4.1.11. informação de que os serviços prestados poderão ser auditados.

14.4.2. Os serviços de terceiros, prestados a Prefeitura de Salvador devem ser monitorados e analisados criticamente de forma regular, a fim de garantir a aderência entre os termos de Segurança da Informação e as condições dos acordos, além de permitir o gerenciamento adequado de problemas e Incidentes de Segurança da Informação.

14.4.3. Devem ser executadas auditorias periódicas nos serviços de terceiros, contemplando, mas não limitando-se a:

14.4.3.1. níveis de desempenho de serviço para verificar aderência aos acordos;

14.4.3.2. relatórios de serviços produzidos por terceiros;

14.4.3.3. registros dos incidentes de Segurança da Informação e de sua respectiva análise crítica, tanto pelo terceiro quanto pelo órgão ou entidade, como requerido pelos acordos e por quaisquer procedimentos e diretrizes que os apoiam;

14.4.3.4. trilhas de auditoria do terceiro e registros de eventos de segurança, problemas operacionais, falhas, investigação de falhas e interrupção relativas ao serviço.

14.4.4. Um processo de gerenciamento de mudanças deve ser elaborado para os serviços prestados por terceiros a fim de garantir que modificações em recursos de Tecnologia da Informação sejam processadas, levando-se em consideração o grau de importância dos sistemas e processos de negócio envolvidos. Este processo deve contemplar, mas não limitando-se a:

14.4.4.1. melhoria dos serviços correntemente oferecidos;

14.4.4.2. desenvolvimento de quaisquer novas aplicações ou sistemas;

14.4.4.3. modificações ou atualizações das políticas e procedimentos;

14.4.4.4. novos controles para resolver os incidentes de Segurança da Informação e melhoria da segurança;

14.4.4.5. mudanças e melhorias em redes;

14.4.4.6. uso de novas tecnologias;

14.4.4.7. adoção de novos produtos ou novas versões;
14.4.4.8. novas ferramentas e ambientes de desenvolvimento;
14.4.4.9. mudanças de localização física dos recursos de serviços;
14.4.4.10. mudanças de fornecedores;
14.4.4.11. mudanças de contratos.

14.5 Competências

14.5.1 Áreas de Negócio do Órgão ou Entidade

14.5.1.1. administrar os contratos sob sua responsabilidade;
14.5.1.2. monitorar e aprovar periodicamente as atividades dos prestadores de serviços, quanto à qualidade e eficiência;
14.5.1.3. avaliar regularmente o direito de acesso dos prestadores de serviço sob sua responsabilidade;
14.5.1.4. comunicar, área de Tecnologia da Informação, infrações aos acordos de segurança estabelecidos por meio de incidentes de Segurança da Informação;
14.5.1.5. auditar periodicamente os serviços de terceiros.

14.5.2 Área de Tecnologia da Informação do Órgão ou Entidade

14.5.2.1. definir, junto as áreas envolvidas, os níveis de entrega de serviços adequados e os requisitos necessários para garantia da segurança das informações;
14.5.2.2. implementar um processo de gerenciamento de mudanças em recursos de Tecnologia da Informação para serviços de terceiros.

14.6 Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2022
- Norma 02 - Classificação da Informação.
- Norma 06 - Gerenciamento de Incidentes de Segurança da Informação.
- Norma 11 - Intercâmbio de Informações.
- Norma 12 - Segurança Física.

14.7 Data de Revisão

18/10/2023

15 Norma 14 - Desenvolvimento e Manutenção de Aplicações

15.1 Objetivo

Estabelecer as diretrizes que regulamentam a segurança para o processo de desenvolvimento e manutenção de software no âmbito da Administração Pública Municipal.

15.2 Definições

Artefato de Software: item criado como parte da definição, manutenção ou utilização de um processo de software, incluindo, entre outros, descrições de processos, planos, procedimentos, especificações, projetos de arquitetura, projeto detalhado, código, documentação para o usuário.

Base de Dados: conjunto de dados organizados de forma a servir de base para que o usuário processe e recupere informações.

Gestão de Configuração: conjunto de procedimentos técnicos e gerenciais que são definidos para identificação de Ativos de Tecnologia da Informação e para a gestão de suas alterações.

Rastreabilidade: capacidade de acompanhamento e registro de todos os eventos e movimentações ocorridas, desde a criação da informação até o seu descarte.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

15.3 Abrangência

Esta Norma se aplica a todos os usuários envolvidos nos processos de desenvolvimento e manutenção de software no âmbito da Administração Pública Municipal.

15.4 Diretrizes

15.4.1. Pelo menos uma metodologia deve ser estabelecida para todo desenvolvimento ou manutenção, com base nas melhores práticas de mercado, contemplando, entre outros:
15.4.1.1. planejamento;
15.4.1.2. análise de requisito;
15.4.1.3. projeto;
15.4.1.4. codificação;
15.4.1.5. revisão;
15.4.1.6. compilação;
15.4.1.7. teste.
15.4.2. Todo desenvolvimento ou manutenção de software deve ser formalmente autorizado.
15.4.3. Para todo desenvolvimento ou manutenção de software deve ser realizada uma análise de impacto.
15.4.4. Toda alteração de escopo de desenvolvimento ou manutenção de software deve ser documentada e formalmente autorizada.
15.4.5. Todas as ferramentas de desenvolvimento devem ser homologadas e licenciadas.
15.4.6. Todo projeto de software deve conter um documento de especificação que descreva seus requisitos de segurança, os quais devem, entre outros, contemplar:
15.4.7. mecanismo de autenticação do usuário, que deve utilizar senhas com métrica mínima e exigir do usuário a troca periódica da senha;

15.4.8. o mecanismo de autenticação do usuário, que deve bloquear o acesso após número definido de tentativas de login com falha;

15.4.9. a verificação da senha por meio de mecanismo que impeça fraudes de repetição, interceptação ou quebra de integridade na comunicação entre o cliente e o servidor;

15.4.10. a escolha da senha por novos usuários sem a interferência do pessoal de apoio ou o recebimento por eles, de uma senha inicial que precise ser trocada;

15.4.11. o armazenamento da senha pelo sistema, de forma criptografada e irreversível;

15.4.12. a uniformidade do controle de acesso em todo o sistema, utilizando-se uma única rotina de verificação;

15.4.13. a realização do controle de acesso na camada mais próxima possível dos dados;

15.4.14. o registro, pelo sistema, dos eventos significativos para a segurança, principalmente, início e fim do mecanismo de auditoria;

15.4.15. o registro, pelo sistema, das falhas de login, indicando o número de tentativas;

15.4.16. o registro, pelo sistema, da criação e remoção de usuários, bem como da atribuição e da remoção de direitos do usuário;

15.4.17. a proteção da trilha de auditoria contra remoção e alteração por parte de todos os usuários, exceto dos administradores de auditoria;

15.4.18. a capacidade de tolerância do sistema a falhas e retorno a operação;

15.4.19. a inexistência, em aplicações web, de dados sensíveis em campos ocultos ou cookies;

15.4.20. a realização das verificações e validações de segurança no servidor, em aplicações web;

15.4.21. o acesso aos desenvolvedores apenas aos códigos fontes necessários para a alteração, quando autorizados pelo superior imediato;

15.4.22. a maior semelhança possível do ambiente de homologação ao ambiente de produção;

15.4.23. a exigência de que os aplicativos só passem do desenvolvimento para a homologação após verificação da existência e adequação de sua documentação;

15.4.24. a existência de documentação de instalação, configuração e operação do sistema, ressaltando os aspectos de segurança, que deve ser mantida atualizada.

15.4.25. Requisitos funcionais, não funcionais e de domínio devem ser especificados e documentados, bem como as manutenções necessárias, considerando os requisitos de segurança definidos no desenvolvimento do sistema.

15.4.26. A especificação dos requisitos deve ser elaborada em conjunto com a área de negócio solicitante da demanda.

15.4.27. Um mecanismo de controle de versão deve ser implementado durante o processo de desenvolvimento e manutenção de software.

15.4.28. Deve existir um programa de conscientização em Segurança da Informação para todos os usuários envolvidos nos processos de desenvolvimento de aplicações.

15.4.29. Devem existir mecanismos de verificação de vulnerabilidades no código fonte durante o processo de desenvolvimento e manutenção de software.

15.4.30. Incidentes de segurança devem ser abertos quando vulnerabilidades forem identificadas durante o processo de desenvolvimento e manutenção de software.

15.4.31. O acesso aos códigos fontes deve ser controlado e restrito aos desenvolvedores envolvidos, em seus respectivos projetos.

15.4.32. Os códigos fontes não devem conter identificações e/ou senhas de acesso às bases de dados, sejam elas de teste, de homologação ou de produção.

15.4.33. Ambientes de desenvolvimento e testes, de homologação e de produção devem ser isolados entre si.

15.4.34. Um processo de gestão de configuração deve ser implementado e deve abranger todo o processo de desenvolvimento e manutenção.

15.4.35. Todo software que implique em manipulação de dados deve ser desenvolvido com controle de acesso lógico. Mecanismos adicionais que possibilitem a rastreabilidade das operações efetuadas devem ser considerados em casos de manipulação de dados sensíveis.

15.5 Desenvolvimento Terceirizado

15.5.1. Todos os contratos com terceiros devem contemplar cláusulas de sigilo e confidencialidade.

15.5.2. Os produtos desenvolvidos externamente devem obedecer a padrões e metodologias homologadas, além de atender aos requisitos funcionais, não funcionais, de domínio e de segurança definidos.

15.5.3. O contrato de desenvolvimento de produtos com terceiros deve prever, no mínimo, os artefatos de software a serem entregues em cada fase, a validação, o procedimento de aceite final e o período de garantia.

15.6 Testes

15.6.1. Procedimentos de testes no software devem ser definidos e utilizados para todo desenvolvimento ou manutenção realizados, e devem contemplar, entre outros, controles tais como:

15.6.1.1. validação de dados de entrada;

15.6.1.2. controle de processamento interno;

15.6.1.3. integridade de mensagens;

15.6.1.4. validação de dados de saída.

15.6.2. Os testes devem validar os mecanismos de segurança especificados no desenvolvimento ou na manutenção do software.

15.6.3. Os testes de aceitação do software devem ser realizados por uma equipe diferente da equipe desenvolvedora, que deve ser composta por usuários da área de desenvolvimento e da área de negócio solicitante.

15.6.4. A utilização de dados de produção em ambiente de testes deve ser autorizada formalmente.

15.6.5. As informações contidas na base de dados de ambiente de produção, se utilizadas para testes, devem sofrer alterações, de modo a preservar sua confidencialidade.

15.7 Aceitação de Software

15.7.1. Os artefatos de software, provenientes de desenvolvimento ou manutenção, devem ser homologados antes de serem utilizados em ambiente de produção.

15.8 Mudanças Técnicas no Ambiente de Produção

15.8.1. As atualizações de configuração no ambiente de produção devem ser realizadas, inicialmente, em ambiente de teste e, todo software deve ser analisado criticamente, considerando os seguintes aspectos:

15.8.1.1. análise crítica dos procedimentos de controle e integridade do software, garantindo que eles não foram comprometidos pelas mudanças efetuadas no ambiente de produção;

15.8.1.2. revisão do planejamento e do orçamento anual para suporte, garantindo investimentos para revisões e testes de softwares resultantes das modificações do ambiente de produção;

15.8.1.3. revisão do Plano de Continuidade dos Negócios para contemplar mudanças necessárias resultantes das modificações do ambiente de produção.

15.9 Implantação

15.9.1. Os produtos homologados devem ser implantados em ambiente de produção, por meio de procedimentos técnicos definidos pela área de Tecnologia da Informação do órgão ou entidade e aceite da área cliente.

15.9.2. Planos de Continuidade Operacional devem ser desenvolvidos pelas áreas de negócio do órgão ou entidade para garantir a continuidade dos processos envolvidos nas implantações de software ou outras mudanças relacionadas.

15.9.3. A implantação de novo software deve ser realizada de acordo com o calendário definido pelas áreas de negócio do órgão ou entidade, com a participação da respectiva área de Tecnologia da Informação.

15.10 Competências

15.10.1 Áreas de Negócio do Órgão ou Entidade:

15.10.1.1. autorizar a utilização de dados de produção no ambiente de testes;

15.10.1.2. elaborar procedimentos de homologação,

15.10.1.3. homologar e dar aceite aos produtos desenvolvidos pela área de Tecnologia da Informação do órgão ou entidade;

15.10.1.4. elaborar Planos de Continuidade Operacional para garantir a continuidade dos processos envolvidos nas implantações de software ou outras mudanças relacionadas.

15.10.2 Área de Tecnologia da Informação do Órgão ou Entidade

15.10.2.1. homologar os procedimentos e metodologias de desenvolvimento externo;

15.10.2.2. definir treinamentos necessários para os desenvolvedores;

15.10.2.3. analisar os impactos das solicitações de desenvolvimento e modificações e autorizar ou realizar o desenvolvimento ou a manutenção;

15.10.2.4. definir procedimentos de testes e implantação de software;

15.10.2.5. realizar testes no software desenvolvido ou modificado;

15.10.2.6. homologar software e ferramentas de desenvolvimento de software;

15.10.2.7. disponibilizar ferramenta para atualizar software no ambiente de produção.

15.11 Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2022
- ISO/IEC 15408-1:2009 Information Technology - Security Techniques -- Evaluation Criteria for IT Security-- Part 1: Introduction and general model.
- ISO/IEC15408-2:2008 Information Tecnology - Security techniques -- Evaluation criteria for IT security—Part 2: Security functional components
- ISO/IEC15408-3:2008 Information Tecnology - Security toxiques -- Evaluation criteria for IT Security—Part3: Security assurance components
- Norma 02 - Classificação da de Informação.
- Norma 10 - Contabilização de Ativos de Tecnologia da Informação.
- Norma 11 - Intercâmbio de Informações.

15.12 Data de Revisão

18/10/2023

16 Norma 15 - Distribuição de Hardware e Software

16.1 Objetivo

Estabelecer diretrizes para a aquisição, distribuição e gerenciamento de hardware e software no âmbito da Administração Pública Municipal.

16.2 Definições

Biblioteca de Software Definitivo: repositório no qual as versões autorizadas e definitivas de todos os itens de software em produção estão armazenadas e protegidas.

Depósito de Hardware Definitivo: área separada para o armazenamento de todos os itens definitivos de hardware sobressalente.

Freeware: programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso.

Processo de Gestão de Mudanças: processo que assegura que métodos e procedimentos padronizados sejam utilizados para um tratamento rápido e eficiente de todas as mudanças, de modo a minimizar o impacto de quaisquer incidentes relacionados aos recursos de Tecnologia da Informação.

Shareware: programa disponível publicamente para avaliação e uso experimental, mas, cujo uso em regime pressupõe que o usuário pagará uma licença ao autor. Shareware é distinto de freeware, no sentido de que um software shareware é comercial, embora em termos e preços diferenciados em relação a um produto comercial convencional.

Software Livre: denominação dada a determinado software cujo código-fonte é de domínio público e, em geral, gratuito.

16.3 Abrangência

Esta Norma se aplica a todos os usuários, processos de negócio, sistemas, serviços e Ativos de Tecnologia da Informação da Administração Pública Municipal.

16.4 Aquisição de Hardware e Software

16.4.1. Toda aquisição de hardware ou software deve ser precedida de um levantamento das necessidades do processo de negócio a que se destinam, tais como: capacidade de processamento, flexibilidade, estrutura de dados, entre outros.

16.4.2. Antes da aquisição de hardware ou software críticos e, quando possível, havendo concordância do fornecedor, deve ser conduzida uma Prova de Conceito (POC –Proof of Concept).

16.4.3. Todos os itens adquiridos devem ser inventariados conforme norma específica (Norma de Contabilização de Ativos de Tecnologia da Informação) e, quando viável, ser apoiado por uma ferramenta de automação.

16.4.4. Períodos de vida útil devem ser definidos para cada tipo de hardware, contemplando as necessidades do processo de negócio a que se destina e o retorno de investimento (ROI) durante seu ciclo de vida.

16.4.5. Planos de atualização de hardware e software devem ser elaborados considerando seu período de vida útil, os requisitos funcionais e técnicos dos processos de negócio e, de acordo com o direcionamento tecnológico da Administração Pública Municipal.

16.5 Distribuição de Hardware e Software

16.5.1. Deve ser estabelecido um processo de gestão de mudanças que contemple todas as atividades de distribuição de hardware e software, tais como: adição, modificação e remoção, com o objetivo de controlar os riscos de impacto aos processos de negócio (paralisação ou queda de desempenho prolongadas ou não programadas).

16.5.2. Este processo deve contemplar, entre outros:

16.5.2.1. planejamento das mudanças em conjunto com as áreas de negócio do órgão ou entidade e outras partes relevantes;

16.5.2.2. documentação de todas as mudanças (requisição de mudança);

16.5.2.3. formalização da aceitação de mudanças;

16.5.2.4. identificação de medidas de reversão ou remediação se a mudança não for bem-sucedida;

16.5.2.5. atualização dos inventários de hardware e software;

16.5.2.6. instalação de um ambiente de testes para a homologação de mudanças críticas antes de aplicá-las em ambiente de produção;

16.5.2.7. análise de impacto à integridade dos dados (modificações em arquivos de dados feitas pelo sistema ou aplicação sem intervenção direta do usuário);

16.5.2.8. proteção à integridade de hardware e software durante instalação, manejo e transporte;

16.5.2.9. treinamento a usuários e administradores e documentação correspondente.

16.5.3. Deve ser implementada uma biblioteca de software definitivo com o objetivo de garantir que somente versões autorizadas estejam sendo utilizadas, devendo conter:

16.5.3.1. versões originais, definitivas e autorizadas de todo software e códigos fonte, quando aplicável;

16.5.3.2. repositório para o armazenamento seguro de todas as cópias originais dos softwares e suas respectivas licenças e direitos de propriedade;

16.5.3.3. estrito controle de licenças com o objetivo de eliminar os softwares não autorizados;

16.5.3.4. informações relativas à suporte técnico, direitos de atualização, entre outras condições contratuais;

16.5.3.5. documentação e manuais relacionados.

16.5.4. O processo de distribuição de software deve, quando cabível, ser apoiado por uma ferramenta da automação.

16.5.5. Deve ser implementado um depósito de hardware definitivo com o objetivo de proteger equipamentos sobressalentes, que devem ser mantidos no nível que os seus correspondentes do ambiente de produção e podem ser utilizados por outros sistemas ou para recuperação de incidentes de grande impacto.

16.5.6. O depósito de hardware definitivo deve conter os respectivos manuais e demais documentos atualizados para cada equipamento.

16.6 Competências

16.6.1 Áreas de Negócio do Órgão ou Entidade

16.6.1.1. requerer as mudanças de acordo com os procedimentos definidos no processo de gestão de mudanças.

16.6.2 Área de Tecnologia da Informação do Órgão ou Entidade:

16.6.2.1. elaborar e manter os inventários de hardware e software;

16.6.2.2. estabelecer os períodos de vida útil de hardware e software;

16.6.2.3. elaborar o plano de atualização de hardware e software;

16.6.2.4. implementar o processo de gestão de mudanças para apoiar a distribuição de hardware e software;

16.6.2.5. avaliar, aprovar e implementar ou negar as requisições de mudança em cooperação com as áreas de negócio envolvidas;

16.6.2.6. promover a melhoria contínua do processo de gestão de mudanças;

16.6.2.7. distribuir os itens de hardware e software;

16.6.2.8. implementar a biblioteca de software definitivo e o depósito de hardware definitivo.

16.7 Documentos Relacionados

- ABNT NBR ISO/IEC 20000-1:2011 - Tecnologia da informação — Gestão de serviços Parte 1: Requisitos do sistema de gestão de serviços
- ABNT NBR ISO/IEC 27002:2022– Tecnologia da Informação – Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação.
- ABNT NBR ISO 31000:2009 - Gestão de Riscos - Princípios e diretrizes.
- ITIL – Information Technology Infrastructure Library.
- Norma 09 - Gerenciamento de Riscos.
- Norma 10 - Contabilização de Ativos de Tecnologia da Informação.
- Norma 14 - Desenvolvimento e Manutenção de Aplicações.

16.8 Data de Revisão

18/10/2023.

17 Norma 16 - Proteção Contra Código Malicioso

17.1 Objetivos

Estabelecer diretrizes para a proteção dos recursos de Tecnologia da Informação da Administração Pública Municipal contra ação de código malicioso, programas impróprios.

17.2 Definições

Código Malicioso: termo genérico que se refere a todos os tipos de programa especificamente desenvolvidos para executar ações danosas em recursos de Tecnologia da Informação, tais como vírus, cavalo de troia, spyware, worms, entre outros.

Log: arquivo que contém informações sobre eventos de qualquer natureza em um sistema computacional, análise forense para a elucidação de incidentes de segurança, auditoria de processos, cumprimento de exigências legais para a manutenção de registro do histórico de acessos ou eventos e para a resolução de problemas (debugging).

Programas Impróprios: programas utilitários utilizados para explorar vulnerabilidades ou burlar a segurança dos recursos de Tecnologia da Informação.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

17.3 Abrangência

Esta Norma se aplica a todos os usuários e recursos de Tecnologia da Informação da Administração Pública Municipal.

17.4 Diretrizes

17.4.1. Os recursos de Tecnologia da Informação devem estar providos de sistemas de detecção e bloqueio de códigos maliciosos, tais como programas antivírus, programas de análise de conteúdo de Correio Eletrônico.

17.4.2. Havendo correções ou atualizações para os sistemas de detecção e bloqueio de códigos maliciosos, as mesmas devem ser implementadas, a fim de se evitar que estes sistemas fiquem vulneráveis a códigos maliciosos ou a qualquer tentativa de acesso não autorizado.

17.4.3. As atualizações e as correções para os sistemas de detecção e bloqueio de programas maliciosos devem ser homologadas antes de aplicadas ao ambiente de produção.

17.4.4. É obrigatório o uso de sistemas de detecção e bloqueio de códigos maliciosos em todos os recursos de Tecnologia da Informação.

17.4.5. Arquivos ou mídias que são utilizados nos equipamentos computacionais devem ser verificados automaticamente, quanto à contaminação por código malicioso, antes de sua utilização.

17.4.6. Os sistemas de detecção e bloqueio de códigos maliciosos devem prover monitoramento, em tempo de execução, dos arquivos e programas, quanto à contaminação por código malicioso.

17.4.7. Os arquivos contaminados por código malicioso devem ser imediatamente descontaminados pelo software antivírus, isolados ou removidos do sistema. Em caso de persistência do problema, o equipamento deve ser isolado até que seja sanado o problema para não afetar o ambiente de produção.

17.4.8. Padrões e procedimentos para instalação, configuração, utilização e atualização de sistemas de detecção e bloqueio de códigos maliciosos devem ser estabelecidos pela área de Tecnologia da Informação do órgão ou entidade.

17.4.9. Somente mídias magnéticas e produtos de origem confiável devem ser utilizados nos equipamentos computacionais.

17.5 Competências

17.5.1 Área de Tecnologia da Informação do Órgão ou Entidade

17.5.1.1. auxiliar no processo de conscientização dos usuários quanto às melhores práticas de prevenção contra códigos maliciosos;

17.5.1.2. garantir a instalação dos sistemas de detecção e bloqueio de programas maliciosos nos equipamentos computacionais, mantendo-os atualizados, conforme disponibilização do fabricante;

17.5.1.3. monitorar os logs dos sistemas de detecção e bloqueio de códigos maliciosos, com objetivo de atuar de forma proativa na identificação de ameaças.

17.5.2 Usuário

17.5.2.1. utilizar somente programas homologados pelo fabricante e devidamente licenciados.

17.6 Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2022– Tecnologia da Informação – Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação.
- Norma 06 - Gerenciamento de Incidentes de Segurança da Informação.

17.7 Data de Revisão

18/10/2023

18 Norma 17 - Uso de Dispositivos Móveis

18.1 Objetivo

Proteger os recursos computacionais disponibilizados pela administração pública do poder executivo municipal contra a ação de códigos maliciosos, códigos móveis e programas impróprios, através da definição de regras, critérios de acesso e soluções visando prevenir incidentes de segurança para a organização.

18.2 Definições

Antivírus: programa (software) especificamente desenvolvido para detectar, anular e eliminar vírus e outros tipos de códigos maliciosos.

BYOD: (Bring Your Own Device – tradução: "traga seu próprio dispositivo") termo utilizado para definição da prática do uso de dispositivos móveis, de propriedade do colaborador, nas instalações físicas da Organização para realização de atividades laborais.

Código Malicioso (malware): termo genérico que se refere a todo tipo de programa especificamente desenvolvido para executar ações danosas em um computador ou outros dispositivos eletrônicos, a exemplo de: vírus, cavalos de tróia, spyware, backdoors, keyloggers, worms, bots e rootkits.

Código Móvel: código executado localmente, proveniente de um sistema remoto de baixa confiabilidade, que executa automaticamente funções específicas com pequena ou nenhuma interação por parte do usuário.

Conformidade: aderência a um padrão previamente estabelecido e aceito como ideal.

Criptografia: técnica utilizada para tornar a informação original ilegível, permitindo que somente o destinatário (detentor da chave de criptografia) a decifre.

Dispositivos Móveis: equipamento ou acessório portátil, capaz de se conectar a internet e/ou armazenar dados, tais como: celular, smartphone, tablet, notebook, pendrive, CD/DVD e outros semelhantes.

Domínio: Referência que define um nome para o serviço de autenticação dos usuários em uma rede. O nome dado ao domínio, normalmente é usado para fazer referência a rede corporativa da organização.

Informação Sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Rede Corporativa: nomenclatura utilizada para definir os serviços e recursos tecnológicos de uma rede vinculados ao negócio da organização, disponibilizados para os usuários que possuem credencial de acesso no domínio da instituição.

Rede Visitante: nomenclatura utilizada para definir uma rede ou segmento de rede, disponibilizada aos usuários visitantes, com serviços limitados e acesso restrito aos serviços e recursos tecnológicos da rede corporativa.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Municipal em local ou jornada de trabalho para este último.

Usuário de dispositivo móvel: todo colaborador seja ele servidor, estagiário ou prestador de serviço que acessa, através de dispositivos móveis, informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Estadual.

Usuário Visitante: Qualquer usuário sem vínculo com o órgão ou entidade da administração pública estadual que necessite acessar, de forma temporária, recursos computacionais da organização. Vulnerabilidade: fragilidade de um software, sistema operacional ou outro componente da infraestrutura de Tecnologia da Informação que pode ser explorada por uma ou mais ameaças internas ou externas à organização.

18.3 Abrangência

Todos os usuários com dispositivos móveis (de propriedade da organização ou próprio) que desejem acessar os recursos computacionais da organização.

18.4 Diretrizes

18.4.1. A fim de viabilizar o cumprimento desta Norma, nos casos em que for permitido o acesso utilizando dispositivo móvel, a organização reserva-se o direito de, através das áreas competentes:

18.4.2. Instalar software ou agente para monitorar a utilização e o acesso dos dispositivos móveis aos recursos computacionais da organização;

18.4.3. Auditar, quando necessário, os dispositivos móveis disponibilizados pela organização; Todos os dispositivos móveis utilizados como estação de trabalho (notebook, tablet, etc.), devem se autenticar no domínio da organização, para ter acesso aos recursos da rede corporativa.

18.4.4. O usuário de dispositivos móveis corporativos, tem responsabilidade sobre todo e qualquer conteúdo armazenado, e pela integridade deles.

18.5 Acesso à Internet

18.5.1. É vedado o uso de modem em equipamento conectado à rede da organização para acesso direto a redes externas, inclusive Internet, nas dependências da organização, salvo para a realização de testes específicos pelas áreas técnicas competentes. O acesso às redes externas deve ocorrer através da arquitetura segura existente e homologada pela organização;

18.5.2. É vedado o uso do serviço de ancoragem / roteamento dos dispositivos móveis com equipamentos conectados à rede corporativa;

18.5.3. Ressalvados os interesses da Administração Pública Municipal é vedado fazer download ou upload de arquivos através dos recursos da organização cuja utilização ou conteúdo não estejam relacionados às atividades profissionais do usuário de dispositivo móvel, especialmente aqueles que possam representar risco à segurança do ambiente operacional da organização, tais como, mas não limitados a:

18.5.3.1. arquivos de áudio e vídeo;

18.5.3.2. arquivos anexados a mensagens cujos remetentes não são identificáveis ou confiáveis;

18.5.3.3. arquivos multimídia;

18.5.3.4. arquivos executáveis.

18.5.4. Todos os usuários que utilizam recursos da organização para acesso à Internet, devem se autenticar na rede visitante.

18.6 Uso Adequado de Dispositivos Móveis Corporativos

18.6.1. Quando conectados à rede corporativa da organização os dispositivos móveis devem ser configurados e utilizados de forma a reduzir a probabilidade de atuação de códigos maliciosos. Desta forma, as seguintes diretrizes devem ser observadas:

18.6.1.1. Os dispositivos móveis devem estar providos de sistemas de detecção e bloqueio de códigos maliciosos e prevenção e detecção de acesso não autorizado;

18.6.1.2. Qualquer dispositivo móvel conectado a uma estação de trabalho deverá ser submetido à verificação do software de antivírus, visando detectar à existência de códigos maliciosos e códigos móveis;

18.6.1.3. Não são permitidos a manipulação e armazenamento de músicas, filmes, fotos e software objeto de direitos autorais sem a devida autorização, ou qualquer outro tipo de operação ilegal semelhante, para os dispositivos móveis pertencentes à organização;

18.6.1.4. Não é permitido o armazenamento de informações consideradas sigilosas, em dispositivos móveis sem a devida proteção de segurança, a exemplo do uso de senhas de acesso ao dispositivo, recursos de criptografia ou outra solução adequada para proteção;

18.6.1.5. Documentos criados fora da rede corporativa deverão ser copiados para o ambiente corporativo;

18.6.1.6. Dispositivos móveis cedidos pela organização devem usar, exclusivamente: software homologado e adequadamente licenciado, ou software gratuito autorizado pela organização.

18.6.2. O simples fato de a organização permitir acesso ou uso do equipamento ou recursos de informação, por si só, não configura sobreaviso ou sobre jornada do usuário de dispositivo móvel, sendo um ato de liberalidade, proatividade e iniciativa dele.

18.7 Uso de dispositivo móveis de propriedade particular

18.7.1. Com base no conceito de BYOD, a organização deve disponibilizar uma solução de gerenciamento de todos os dispositivos móveis que acessem os recursos computacionais da organização;

18.7.2. Nos casos em que o usuário de dispositivo móvel utilize seu equipamento no ambiente de trabalho com fins laborais deverão ser obedecidas as condições e diretrizes de segurança da informação descritas a seguir:

18.7.2.1. O proprietário do equipamento assumirá a responsabilidade por:

18.7.2.1.1.1. Conteúdo dos arquivos armazenados;

18.7.2.1.1.2. Licenciamento regular dos softwares instalados, sob pena de responder isoladamente pelo seu uso ilegal;

18.7.2.1.1.3. Não utilizar software licenciado para uso não comercial, para manipular dados ou informações da organização, sob pena de responder isoladamente pelo seu uso ilegal;

18.7.2.1.1.4. Sempre utilizar e atualizar os documentos no ambiente da rede corporativa;

18.7.2.2. O equipamento estará sujeito a monitoramento e auditoria por parte da organização;

18.7.2.3. O equipamento estará à disposição da organização como beneficiária de uso temporário e parcial, sem que isso gere qualquer ônus ou responsabilidade para a referida organização;

18.7.2.4. A organização não será responsabilizada pela perda, deterioração, furto, extravio ou quebra do equipamento, e se isso vier a ocorrer o proprietário deverá avisar à organização imediatamente;

18.7.2.5. A organização não será responsável por realizar manutenções, troca de peças, consertos do equipamento e suas funcionalidades. Estas atividades são de completa responsabilidade do proprietário, salvo interesses da administração pública municipal nas situações de softwares corporativos;

18.8 Usuários visitantes com dispositivos móveis

18.8.1. Devem ser estabelecidos procedimentos de controle e concessão de acesso a visitantes que durante a permanência em instalações de órgãos e entidades da administração pública municipal, necessitem conectar seus dispositivos móveis à rede da organização;

18.8.2. Para ter acesso à rede sem fio o usuário visitante deve ser identificado de forma única.

18.9 Termo de Uso e Responsabilidade

18.9.1. Os usuários devem ser orientados a respeito dos procedimentos de segurança acerca dos dispositivos móveis corporativos que lhes forem disponibilizados, mediante a assinatura de Termo de Uso e Responsabilidade do órgão ou entidade a que pertencem.

18.9.2. Não será admitida a alegação de seu desconhecimento nos casos de uso indevido.

18.10 Competências

18.10.1 Área de Tecnologia da Informação do Órgão ou Entidade

18.10.1.1. Propor, disseminar e atualizar as diretrizes sobre o uso de dispositivos móveis nas instalações da organização;

18.10.1.2. Acompanhar e recomendar a adoção de medidas e procedimentos de segurança, visando assegurar o uso adequado de dispositivos móveis na organização;

18.10.1.3. prover os recursos necessários ao cumprimento desta Norma.

18.10.2 Gestor da Área do Usuário

18.10.2.1. comunicar à área de tecnologia da informação do órgão ou entidade todas as movimentações de pessoal que impliquem em concessão, mudança ou revogação de acessos;

18.10.2.2. comunicar à área de Tecnologia da informação do órgão ou entidade sempre que tomar ciência de direitos de acesso desnecessários à execução das atividades por parte de seus subordinados ou de terceiros.

18.10.3 Usuários

18.10.3.1. Utilizar adequadamente os dispositivos móveis conectados na rede da organização, tomando os cuidados necessários para tal, conforme diretrizes estabelecidas nesta Norma.

18.10.3.2. Comunicar, imediatamente, à área de atendimento ao usuário sobre qualquer ocorrência de perda ou avaria do dispositivo móvel.

18.10.3.3. Cumprir com os requisitos de segurança estabelecidos nesta Norma.

18.10.3.4. Manter, de forma adequada, todos os dispositivos móveis sob sua responsabilidade, sendo responsável por todo e qualquer conteúdo armazenado.

18.11 Documentos relacionados

- ABNT NBR ISO/IEC 27002:2022– Tecnologia da Informação – Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação.
- Norma 03 - Uso da Internet.
- Norma 05 - Acesso e Utilização do Correio Eletrônico.

18.12 Data de Revisão

18/10/2023

ANEXO III

SALVADOR
PREFEITURA

Plano Tático de Segurança da Informação

Documento de Normas Administrativas

COGEL/DITEC/GSE
V 1.0

Histórico de revisões

COGEL Companhia de Governança Eletrônica de Salvador / SALVADOR PREFEITURA / GS	
Plano tático de Segurança da Informação da PMS	*Versão: 1.0*
	Data: 15/08/2023
Publicação	*COGEL/DITEC/GSE*

Histórico de Versões	Data	Alteração
Versão 1.0	18/10/2023	Primeira versão do PTS adequada a norma ISO/IEC 27002:2022

Sumário

1 Introdução 5
2 Controles Organizacionais 5
2.1.1 A5.1 Políticas de Segurança da Informação....5
2.1.2 A5.2 Papeis e Responsabilidades pela Segurança da Informação....5
2.1.3 A5.3 Segregação de Funções....6
2.1.4 A5.4 Responsabilidades da Alta Direção....6
2.1.5 A5.5 Contato com autoridades legais 6
2.1.6 A5.6 Contato com grupos de interesse especial em segurança 6
2.1.7 A5.7 Inteligência de ameaças 6
2.1.8 A5.8 Segurança da informação no gerenciamento de projetos 7
2.1.9 A5.9 Inventário do ativo de informações e outros ativos associados....7
2.1.10 A5.10 Uso aceitável de informações e outros ativos associados....7
2.1.11 A5.11 Devolução de ativos....7
2.1.12 A5.12 Classificação das informações 7
2.1.13 A5.13 Rotulagem das informações 8
2.1.14 A5.14 Transferência de informações 8
2.1.15 A5.15 Controle de acesso 8
2.1.16 A5.16 Gestão de identidade....8
2.1.17 A5.17 Informações de autenticação....9
2.1.18 A5.18 Direitos de acesso 9
2.1.19 A5.19 Segurança da informação nas relações com fornecedores....9
2.1.20 A5.20 Abordagem da segurança da informação nos contratos de fornecedores 9
2.1.21 A5.21 Gestão da segurança da informação na cadeia de fornecimento de TIC 9
2.1.22 A5.22 Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores 10
2.1.23 A5.23 Segurança da Informação para serviços em nuvem....10
2.1.24 A5.24 Planejamento e preparação da gestão de incidentes de segurança da informação 10
2.1.25 A5.25 Avaliação e decisão sobre eventos de segurança da informação....10
2.1.26 A5.26 Resposta a incidentes de segurança da informação 10
2.1.27 A5.27 Aprendizado com incidentes de segurança da informação 11
2.1.28 A5.28 Coleta de evidências....11
2.1.29 A5.29 Segurança da informação durante a interrupção dos serviços....11
2.1.30 A5.30 Prontidão de TIC para continuidade de negócios 11
2.1.31 A5.31 Requisitos legais, estatutários, regulamentares e contratuais....11
2.1.32 A5.32 Direitos de propriedade intelectual 12
2.1.33 A5.33 Proteção de registros....12
2.1.34 A5.34 Proteção e Privacidade de Dados Pessoais 12
2.1.35 A5.35 Análise crítica independente da segurança da informação 12
2.1.36 A5.36 Conformidade com políticas, regras e normas para a segurança da informação 13
2.1.37 A5.37 Documentação dos procedimentos de operação....13
3 Controle de Pessoas 13
3.1.1 A6.1 Verificações....13
3.1.2 A6.2 Termos e condições de contratação 13
3.1.3 A6.3 Conscientização , educação e treinamento em segurança da informação 14
3.1.4 A6.4 Processo disciplinar 14
3.1.5 A6.5 Responsabilidade após encerramento ou mudança da contratação....14
3.1.6 A6.6 Acordos de confidencialidade ou não divulgação 14
3.1.7 A6.7 Trabalho remoto....14
3.1.8 A6.8 Relatos de eventos de segurança da informação....15
4 Controles Físicos 15
4.1.1 A7.1 Perímetros de segurança física....15
4.1.2 A7.2 Entrada Física....15
4.1.3 A7.3 Segurança de escritórios, salas e instalações 15
4.1.4 A7.4 Monitoramento de segurança física 16
4.1.5 A7.5 Proteção contra ameaças físicas e ambientais....16
4.1.6 A7.6 Trabalho em áreas seguras....16
4.1.7 A7.7 Mesa limpa e tela limpa 16
4.1.8 A7.8 Localização e proteção de equipamentos....16
4.1.9 A7.9 Segurança de ativos fora das instalações da organização....17
4.1.10 A7.10 Mídia de armazenamento....17
4.1.11 A7.11 Serviços de infraestrutura....17
4.1.12 A7.12 Segurança de cabeamento....17
4.1.13 A7.13 Manutenção de equipamentos 17
4.1.14 A7.14 Descarte seguro ou reutilização de equipamentos 18
5 Controles Tecnológicos 18
5.1.1 A8.1 Dispositivos endpoint do usuário....18
5.1.2 A8.2 Direitos de acessos privilegiados 18
5.1.3 A8.3 Restrição de acesso a informação 18
5.1.4 A8.4 Acesso ao código fonte....18
5.1.5 A8.5 Autenticação segura 19
5.1.6 A8.6 Gestão da capacidade....19
5.1.7 A8.7 Proteção contra malware....19
5.1.8 A8.8 Gestão de vulnerabilidades técnicas....19
5.1.9 A8.9 Gestão de configuração....19
5.1.10 A8.10 Exclusão de informações....20
5.1.11 A8.11 Mascaramento de Dados....20
5.1.12 A8.12 Prevenção de vazamento de dados 20
5.1.13 A8.13 Cópia de Segurança (Backup) das informações....20
5.1.14 A8.14 Redundância dos recursos de tratamento das informações....20
5.1.15 A8.15 Log 21
5.1.16 A8.16 Atividades de monitoramento 21
5.1.17 A8.17 Sincronização do relógio 21
5.1.18 A8.18 Uso de programas utilitários privilegiados....21
5.1.19 A8.19 Instalação de software em sistemas operacionais....21
5.1.20 A8.20 Segurança de redes....22
5.1.21 A8.21 Segurança dos serviços de rede 22
5.1.22 A8.22 Segregação de redes....22
5.1.23 A8.23 Filtragem da Web....22
5.1.24 A8.24 Uso de criptografia....22
5.1.25 A8.25 Ciclo de vida do desenvolvimento seguro 23
5.1.26 A8.26 Requisitos de segurança do aplicativo 23
5.1.27 A8.27 Princípios de seguros de arquitetura e engenharia de sistemas 23
5.1.28 A8.28 Codificação segura 23
5.1.29 A8.29 Testes de segurança em desenvolvimento e aceitação 23
5.1.30 A8.30 Desenvolvimento terceirizado....24
5.1.31 A8.31 Separação dos ambientes de desenvolvimento, teste e produção 24
5.1.32 A8.32 Gestão de mudanças....24
5.1.33 A8.33 Informações de Teste 24
5.1.34 A8.34 Proteção de sistemas de informação durante os testes de auditoria 24

1 Introdução

A COGEL/DITEC, através da Assessoria de Segurança Cibernética e da Gerência Especial de Segurança (GES) são as responsáveis por gerenciar os recursos disponíveis na PMS voltados para a Segurança da Informação e as suas capacidades operacionais.

As capacidades operacionais envolvem a Governança, Gerenciamento de ativos, Proteção da informação, Segurança de recursos humanos, Segurança física, Segurança de sistemas e redes, Segurança de aplicativos, Configuração de indicadores, Gerenciamento de identidade e acesso, Gerenciamento de ameaças e vulnerabilidades, Continuidade dos negócios, Segurança de relacionamento com fornecedores, Jurídico, Conformidade, Gerenciamento de incidentes e Garantia de continuidade dos negócios.

A norma NBR ISSO/IEC 27001:2022 , em conformidade com a legislação vigente no Brasil e com base nas recomendações da ABNT NBR ISO / IEC 27002:2022, orientam procedimentos para a Gestão da Segurança da Informação através da implementação dos seguintes controles de segurança da informação:

- Controles Organizacionais: políticas, procedimentos e estruturas organizacionais implementados para gerenciar e proteger os recursos de TI;
- Controle de Pessoas: medidas tomadas para garantir que apenas pessoas autorizadas tenham acesso aos recursos de TI;
- Controles Físicos: medidas de segurança física implementadas para proteger os recursos de TI da empresa;
- Controles Tecnológicos: medidas de segurança da informação implementadas por meio de ferramentas e recursos de TI.
-

2 Controles Organizacionais

Contemplam políticas, procedimentos e estruturas organizacionais implementados para gerenciar e proteger os recursos de TI. A norma NBR ISO/IEC 27002:2022 orienta a adoção de 37 (trinta e sete) controles organizacionais, codificados a partir da nomenclatura “A5”.

2.1.1 A5.1 Políticas de Segurança da Informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema,#Resiliência

CONTROLE: A política de segurança da informação e as políticas de temas específicos estabelecem a abordagem para gerenciar a segurança da informação na PMS. Elas devem ser aprovadas pela direção da COGEL, publicadas, comunicadas e reconhecidas pelas partes interessadas relevantes.

PROPÓSITO: Assegurar a adequação contínua, efetividade da direção de gestão e suporte a segurança da informação de acordo com os requisitos legais, estatutários, regulatórios e contratais.

2.1.2 A5.2 Papeis e Responsabilidades pela Segurança da Informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema, #Proteção, #Resiliência

CONTROLE: Identificar, elaborar e manter uma “Matriz de Responsabilidade” com o objetivo de identificar as áreas responsáveis e os respectivos titulares que lidam com as questões de gestão da informação na COGEL, incluindo os sistemas corporativos da PMS e os sistemas de cada secretaria mantidos nos servidores da COGEL.

PROPÓSITO: Compreender a estrutura da organização para facilitar o contato com os responsáveis para a implementação, operação e gestão da segurança da informação na PMS.

2.1.3 A5.3 Segregação de Funções

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Governança #Identidade e Acesso

CONTROLE: Elaborar uma Matriz RACI (Requisita, Aprova, Comunica, Implementa) para segregar funções e não estabelecer um domínio de todas as funções por apenas um colaborador e que não seja concedido poderes para execução de tarefas conflitantes.
PROPÓSITO: Evitar possibilidades de fraudes. Permitir controles como monitoramento de atividades, trilhas de auditoria e supervisão gerencial.

2.1.4 A5.4 Responsabilidades da Alta Direção

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança #Ecosistema

CONTROLE: Exigir que os colaboradores apliquem a segurança da informação de acordo com a política de segurança estabelecida. Apoiar os projetos de segurança da informação com todos os recursos necessários. Produzir material de divulgação da direção da COGEL para demonstrar o compromisso com a segurança da informação.
PROPÓSITO: Garantir que a direção entenda seu papel na segurança da informação e realize ações com o objetivo de garantir que todos os funcionários estejam cientes e que cumpram suas responsabilidades.

2.1.5 A5.5 Contato com autoridades legais

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo #Corretivo	#Confidencialidade #integridade #Disponibilidade	#Identificar #Proteger #Responder, #Recuperar	#Defesa, #Resiliência

CONTROLE: Estabelecer e manter contato com autoridades competentes para tratar de questões legais referentes a segurança da informação. Especificar quando e por quem as autoridades devem ser contatadas e como os incidentes identificados de segurança da informação devem ser relatados em tempo hábil.
PROPÓSITO: Garantir o fluxo adequado de informações referentes à segurança da informação entre a PMS e as autoridades legais, regulatórias e fiscalizadoras relevantes.

2.1.6 A5.6 Contato com grupos de interesse especial em segurança

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo #Corretivo	#Confidencialidade #integridade #Disponibilidade	#Proteger #Responder #Recuperar	#Defesa

CONTROLE: Estabelecer e manter contato permanente com grupos de especialistas, fóruns de especialistas em segurança e entidades que estudam o tema.
PROPÓSITO: Compartilhar experiências, tecnologias e outras formas de prevenção em segurança da informação para troca de informações.

2.1.7 A5.7 Inteligência de ameaças

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo #Detectivo #Corretivo	#Confidencialidade #integridade #Disponibilidade	#Responder #Identificar #Detectar	#Defesa, #Resiliência

CONTROLE: Detectar os principais tipos de ameaças para realizar análise de riscos e impactos. Estabelecer estratégia de defesa. Realizar testes de intrusão e de ataques simulados através de equipe vermelha (Red Teams). Implementar repositório de ameaças conhecidas.

PROPÓSITO: Conhecer as principais ameaças relativas à segurança para prevenção e resposta a ataques.

2.1.8 A5.8 Segurança da informação no gerenciamento de projetos

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar #Proteger	#Governança, #Ecosistema,#Proteção

CONTROLE: Estabelecer requisitos de segurança para o desenvolvimento de sistemas e ou aquisição de sistemas e aplicativos para a PMS. Estabelecer regras de segurança a serem estabelecidas nos projetos de sistemas.
PROPÓSITO: Preservar os requisitos de segurança mínimos necessários para proteção dos sistemas e avaliação de incidentes relativos à segurança da informação.

2.1.9 A5.9 Inventário do ativo de informações e outros ativos associados

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema,#Proteção

CONTROLE: Elaborar e manter um inventário dos ativos de informação estabelecendo classificação para o ativo e risco envolvido.
PROPÓSITO: Identificar os ativos da PMS, a fim de preservar a sua segurança e atribuir a propriedade apropriada.

2.1.10 A5.10 Uso aceitável de informações e outros ativos associados

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Governança, #Ecosistema,#Proteção

CONTROLE: Estabelecer regras para o uso aceitável dos ativos e procedimentos para o manuseio de informações para que eles sejam identificados, documentados e implementados. Estabelecer regras e responsabilidades pelos ativos de informação.
PROPÓSITO: Assegurar que os ativos e as informações sejam corretamente protegidos, usados e utilizados.

2.1.11 A5.11 Devolução de ativos

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Estabelecer controle dos bens de informação em posse de colaboradores e terceiros e controlar sua devolução em caso de rescisão de contrato.
PROPÓSITO: Proteger os ativos da PMS como parte do processo de mudança ou rescisão do emprego ou contrato.

2.1.12 A5.12 Classificação das informações

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Proteção, #Defesa

CONTROLE: Classificar as informações de acordo com as necessidades de segurança da informação da PMS com base na confidencialidade, integridade, disponibilidade e requisitos relevantes das partes interessadas.
PROPÓSITO: Assegurar a identificação e o entendimento das necessidades de proteção da informação de acordo com a importância para a PMS levando-se em conta o nível de risco e impacto.

2.1.13 A5.13 Rotulagem das informações

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Defesa, #Proteção

CONTROLE: Rotulagem de informações de acordo com o esquema de classificação das informações Exemplos de técnicas de rotulagem: Rótulos físicos, cabeçalhos e rodapés, metadados. Marca d'água, carimbos.
PROPÓSITO: Facilitar a comunicação da classificação de informações e apoio a automação da gestão e processamento das informações.

2.1.14 A5.14 Transferência de informações

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Estabelecer regras e procedimentos ou acordos de transferência de informações entre a organização e outras partes interessadas.
PROPÓSITO: Manter a segurança das informações transferidas dentro da PMS e com qualquer parte interessada.

2.1.15 A5.15 Controle de acesso

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Estabelecer regras para controlar o acesso físico e lógico às informações e outros ativos associados. Estabelecer procedimentos para solicitações formais de acesso aos ativos informacionais.
PROPÓSITO: Assegurar o acesso autorizado e evitar o acesso não autorizado a informações e outros ativos associados.

2.1.16 A5.16 Gestão de identidade

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Gerenciar o ciclo de vida completo das identidades. Atribuir, desativar ou remover identidades que não são mais necessárias a PMS.
PROPÓSITO: Permitir a identificação única de indivíduos e sistemas que acessam a PMS e permitir a cessão adequada de direitos de acesso.

2.1.17 A5.17 Informações de autenticação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Gerenciar as informações de autenticação em ativos de informação. Estabelecer um processo de gestão de autenticação.
PROPÓSITO: Garantir a autenticação adequada da entidade e evitar falhas nos processos de autenticação.

2.1.18 A5.18 Direitos de acesso

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Analisar criticamente junto aos proprietários da informação, da relação de acessos vigentes para que sejam modificados e removidos de acordo com as regras de autorização.
PROPÓSITO: Assegurar que o acesso às informações esteja definido e autorizado de acordo com as exigências do negócio.

2.1.19 A5.19 Segurança da informação nas relações com fornecedores

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema,#Proteção

CONTROLE: Definir processos e procedimentos para gerenciar a segurança da informação e os riscos associados nas relações com os fornecedores.
PROPÓSITO: Manter um nível acordado de segurança da informação nas relações com fornecedores.

2.1.20 A5.20 Abordagem da segurança da informação nos contratos de fornecedores

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema,#Proteção

CONTROLE: Estabelecer requisitos de segurança da informação com base no tipo de relacionamento.
PROPÓSITO: Estabelecer acordos com fornecedores e documentá-los para assegurar que haja um entendimento claro entre a PMS e o fornecedor sobre as obrigações e responsabilidade de ambas as partes em relação a segurança da informação.

2.1.21 A5.21 Gestão da segurança da informação na cadeia de fornecimento de TIC

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema,#Proteção

CONTROLE: Definir e implementar processos e procedimentos para gerenciar riscos de segurança da informação associados a cadeia de fornecimento de produtos e serviços de TIC, a

exemplo de Serviços em nuvem, IoT, aplicativos móveis e web. Observar a norma ISSO/IEC 27036-3 e ISSO/IEC 19770-2.
PROPÓSITO: Manter um nível acordado de segurança da informação nas relações com fornecedores.

2.1.22 A5.22 Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema,#Proteção #Defesa, #Assegurar

CONTROLE: Monitorar, analisar criticamente, avaliar e gerenciar regularmente as práticas de segurança da informação nos fornecedores e na prestação dos serviços.
PROPÓSITO: Manter um nível acordado de segurança da informação e prestação de serviços em linha com os acordos com os fornecedores.

2.1.23 A5.23 Segurança da Informação para serviços em nuvem

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Governança, #Ecosistema,#Proteção

CONTROLE: Estabelecer acordos de aquisição, uso, gerenciamento e saída de serviços em nuvem de acordo com os requisitos de segurança da informação.
PROPÓSITO: Especificar e gerenciar a segurança da informação para o uso de serviços em nuvem.

2.1.24 A5.24 Planejamento e preparação da gestão de incidentes de segurança da informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Corretivo	#Confidencialidade #integridade #Disponibilidade	#Responder, #Recuperar	#Defesa

CONTROLE: Planejar e preparar para gerenciar incidentes de segurança da informação definindo, estabelecendo e comunicando processos. Funções e responsabilidades de gerenciamento de incides de segurança da informação.
PROPÓSITO: Garantir uma resposta rápida, eficaz, consistente e ordenada aos incidentes de segurança da informação, incluindo a comunicação às partes interessadas.

2.1.25 A5.25 Avaliação e decisão sobre eventos de segurança da informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Detecção	#Confidencialidade #integridade #Disponibilidade	#Detectar #Responder	#Defesa

CONTROLE: Avaliar e categorizar os eventos de segurança da informação.
PROPÓSITO: Assegurar a efetiva categorização e priorização de eventos de segurança da informação.

2.1.26 A5.26 Resposta a incidentes de segurança da informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Corretivo	#Confidencialidade #integridade #Disponibilidade	#Responder #Recuperar	#Defesa

CONTROLE: Responder os incidentes de segurança da informação de acordo com os procedimentos documentados. Consultar a ISSO/IEC 27035.
PROPÓSITO: Assegurar resposta eficiente e eficaz aos incidentes de segurança da informação.

2.1.27 A5.27 Aprendizado com incidentes de segurança da informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar #Proteger	#Defesa

CONTROLE: Registrar o aprendizado adquirido com incidentes de segurança da informação para melhorar os controles.
PROPÓSITO: Reduzir a probabilidade ou as consequências de futuros incidentes.

2.1.28 A5.28 Coleta de evidências

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Detectar #Responder	#Defesa

CONTROLE: Estabelecer e implementar procedimentos para identificação, coleta, aquisição e preservação de evidências relacionada a eventos de segurança da informação.
PROPÓSITO: Assegurar uma gestão consistente e eficaz das evidências relacionadas a incidentes de segurança da informação para fins de ações disciplinares e legais.

2.1.29 A5.29 Segurança da informação durante a interrupção dos serviços

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo #Corretivo	#Confidencialidade #integridade #Disponibilidade	#Proteger #Responder	#Resiliência, #Proteção

CONTROLE: Planejar como manter a segurança da informação em um nível apropriado durante a interrupção, estabelecendo sistemas e ferramentas de suporte. Elaborar Plano de continuidade de negócios. Definir controles de compensação para controles de segurança da informação que não podem ser mantidos durante a ruptura.
PROPÓSITO: Proteger as informações e outros ativos associados durante uma interrupção.

2.1.30 A5.30 Prontidão de TIC para continuidade de negócios

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Corretiva	#Disponibilidade	#Continuidade	#Resiliência

CONTROLE: Planejar e implementar testes de continuidade dos negócios. Realizar a Análise de Impacto nos Negócios (BIA), identificando atividades priorizadas que devem ser atribuídas a um Objetivo de Tempo de recuperação (RTO) e os Objetivos de Ponto de recuperação (RPO).
PROPÓSITO: Garantir a disponibilidade das informações e outros ativos de informação durante ruptura.

2.1.31 A5.31 Requisitos legais, estatutários, regulamentares e contratuais

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema,#Proteção

CONTROLE: Identificar, documentar e atualizar requisitos legais, estatutários, regulatórios e contratuais pertinentes a segurança da informação e à abordagem da organização. Definir e documentar os processos específicos e responsabilidade individuais para atender aos requisitos obrigatórios.
PROPÓSITO: Assegurar o cumprimento dos requisitos legais, estatutários, regulatórios e contratuais relacionados à segurança da informação.

2.1.32 A5.32 Direitos de propriedade intelectual

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema

CONTROLE: Implementar procedimentos adequados para proteger os direitos de propriedade intelectual. Publicar procedimentos para a conformidade com os direitos de propriedade que definam o uso adequado de softwares e produtos de informação. Manter registro dos ativos e das licenças, manuais e outros documentos relativos. Realizar revisões para assegurar o uso adequado das licenças.
PROPÓSITO: Assegurar o cumprimento dos requisitos legais, estatutários, regulatórios e contratuais relacionados aos direitos de propriedade intelectual e ao uso de produtos proprietários.

2.1.33 A5.33 Proteção de registros

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar #Proteger	#Defesa

CONTROLE: Implementar controles para proteger registros contra perdas, destruição, falsificação, acesso não autorizado e liberação não autorizada. Emitir diretrizes sobre o armazenamento, manuseio da cadeia de custódia e eliminação de registros. Elaborar cronograma de retenção definindo registros e o período pelo qual eles dev. ser retidos. Observar a publicação DIS 23751:2021.
PROPÓSITO: Assegurar o cumprimento dos requisitos legais, estatutários, regulatórios e contratuais de acordo com as expectativas comunitárias ou sociais relacionadas à proteção e disponibilidade de registros.

2.1.34 A5.34 Proteção e Privacidade de Dados Pessoais

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar #Proteger	#Proteção

CONTROLE: Identificar e atender aos requisitos relativos à preservação da privacidade e proteção de dados pessoais definidos na LGPD. Observar a NBR ISO/IEC 27701, 27018, 27005 e 29134.
PROPÓSITO: Assegurar o cumprimento da LGPD.

2.1.35 A5.35 Análise crítica independente da segurança da informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo #Corretivo	#Confidencialidade #integridade #Disponibilidade	#Identificar #Proteger	#Governança, #Ecosistema

CONTROLE: Analisar criticamente e de forma independente, a abordagem da organização para gerenciar a segurança da informação e sua implementação, em intervalos planejados ou quando ocorrerem mudanças significativas. Realizar auditorias internas e externas.
PROPÓSITO: Assegurar a continua adequação, suficiência e eficácia da abordagem da organização para o gerenciamento da segurança da informação.

2.1.36 A5.36 Conformidade com políticas, regras e normas para a segurança da informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar #Proteger	#Governança, #Ecosistema

CONTROLE: Analisar criticamente a conformidade da política de segurança da informação com a política, regras e normas específicas.
PROPÓSITO: Assegurar que a segurança da informação seja implementada e operada de acordo com a política de segurança da informação da PMS.

2.1.37 A5.37 Documentação dos procedimentos de operação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo #Corretivo	#Confidencialidade #integridade #Disponibilidade	#Proteger, #Recuperar	#Governança, #Ecosistema,#Proteção, #Defesa

CONTROLE: Documentar os procedimentos de operação dos recursos de processamento da informação e disponibilizar para os usuários que o necessitem.
PROPÓSITO: Assegurar o funcionamento correto e seguro dos recursos de processamento da informação.

3 Controle de Pessoas

Contemplam medidas para garantir que apenas pessoas autorizadas tenham acesso aos recursos de TI. A norma NBR ISO/IEC 27.002:2022 orienta a adoção de 8 (oito) controles organizacionais, codificados a partir da nomenclatura “A6”.

3.1.1 A6.1 Verificações

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Governança, #Ecosistema

CONTROLE: Verificar os antecedentes de todos os candidatos antes de ingressar na PMS.
PROPÓSITO: Assegurar que todas as pessoas sejam elegíveis e adequadas para as funções e para as quais são consideradas e permaneçam elegíveis e adequados durante seu emprego.

3.1.2 A6.2 Termos e condições de contratação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Governança, #Ecosistema

CONTROLE: Estabelecer cláusulas e responsabilidade do pessoal e da organização para a segurança da informação.
PROPÓSITO: Garantir que o pessoal entenda suas responsabilidades de segurança da informação para as funções para as quais eles são contratados.

3.1.3 A6.3 Conscientização , educação e treinamento em segurança da informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Governança, #Ecosistema

CONTROLE: Fornecer treinamento, educação e conscientização em segurança da informação regulares em relação política de segurança da informação, políticas e procedimentos de utilização de equipamentos de TI e de telecomunicações nas dependências da PMS.
PROPÓSITO: Assegurar que o pessoal e as partes interessadas estejam cientes e cumpram com suas responsabilidades de segurança da informação.

3.1.4 A6.4 Processo disciplinar

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema,#Resiliência

CONTROLE: Estabelecer regras e procedimentos para que um processo disciplinar seja formalizado e comunicado para tomar ações contra pessoas e outras partes interessadas relevantes que tenham cometido uma violação da política de segurança da informação.
PROPÓSITO: Assegurar que o processo disciplinar seja iniciado somente após a confirmação de que ocorreu uma violação da política de segurança da informação.

3.1.5 A6.5 Responsabilidade após encerramento ou mudança da contratação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Governança, #Ecosistema

CONTROLE: Definir responsabilidades e deveres de segurança da informação que permanecerão válidas após o encerramento ou mudança de contratação.
PROPÓSITO: Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

3.1.6 A6.6 Acordos de confidencialidade ou não divulgação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Governança, #Ecosistema

CONTROLE: Definir acordos de confidencialidade ou não divulgação que reflitam as necessidades da organização para a proteção das informações.
PROPÓSITO: Manter a confidencialidade das informações acessíveis por pessoas ou partes externas.

3.1.7 A6.7 Trabalho remoto

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema,#Resiliência

CONTROLE: Estabelecer medidas de segurança quando as pessoas estiverem trabalhando remotamente.

PROPÓSITO: Assegurar a segurança das informações quando as pessoas estão trabalhando remotamente.

3.1.8 A6.8 Relatos de eventos de segurança da informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Detectivo	#Confidencialidade #integridade #Disponibilidade	#Detectar	#Defesa

CONTROLE: Fornecer mecanismos para que as pessoas relatem eventos de segurança da informação observados ou suspeitos através de canais apropriados em tempo hábil.
PROPÓSITO: Oferecer suporte a relatos consistentes e oportunos relativos a eventos de segurança da informação para que possam ser prevenidos ou minimizar os seus efeitos.

4 Controles Físicos

Contemplam medidas de segurança física implementadas para proteger os recursos de TI da empresa. A norma NBR ISO/IEC 27.002:2022 orienta a adoção de 14 (catorze) controles organizacionais, codificados a partir da nomenclatura "A7".

4.1.1 A7.1 Perímetros de segurança física

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Definir áreas seguras e protegidas por controles de entrada e pontos de acesso apropriados.
PROPÓSITO: Garantir que ocorra apenas acesso físico autorizado às informações da organização e outros ativos associados.

4.1.2 A7.2 Entrada Física

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Proteger áreas através de controles de entrada e pontos de acesso apropriados.
PROPÓSITO: Evitar acesso físico não autorizado.

4.1.3 A7.3 Segurança de escritórios, salas e instalações

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Governança, #Ecosistema,#Resiliência

CONTROLE: Estabelecer procedimentos de segurança física para instalações que trabalham com ativos de informação. Manter sob guarda confidencial informações sobre credenciais de acesso.
PROPÓSITO: Evitar aceso físico não autorizado em salas e instalações.

4.1.4 A7.4 Monitoramento de segurança física

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo, #Detectivo	#Confidencialidade #integridade #Disponibilidade	#Proteger, #Detectar	#Proteção, #Defesa

CONTROLE: Instalar equipamentos de monitoramento continuamente para acesso físico de acesso restrito.
PROPÓSITO: Detectar e impedir o acesso físico não autorizado.

4.1.5 A7.5 Proteção contra ameaças físicas e ambientais

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Projetar e implementar medidas para proteção contra ameaças físicas e ambientais, como desastres naturais e outras ameaças físicas intencionais ou não intencionais à infraestrutura.
PROPÓSITO: Prevenir ou reduzir as consequências de eventos originários de ameaças físicas e ambientais.

4.1.6 A7.6 Trabalho em áreas seguras

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Projetar e implementar medidas de segurança para trabalhar em áreas seguras.
PROPÓSITO: Proteger as informações e outros ativos associados em áreas seguras contra danos e interferência não autorizada do pessoal que trabalha nessas áreas.

4.1.7 A7.7 Mesa limpa e tela limpa

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade	#Proteger	#Proteção

CONTROLE: Estabelecer e aplicar regras de mesa limpa para documentos impressos e mídia de armazenamento removível e regras de tela limpa para os recursos de processamento das informações.
PROPÓSITO: Reduzir os riscos de acesso não autorizado, perda e danos às informações em mesas, telas e em outros locais acessíveis durante e fora do horário de trabalho.

4.1.8 A7.8 Localização e proteção de equipamentos

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Posicionar os equipamentos com segurança e proteção.
PROPÓSITO: Reduzir os riscos de ameaças físicas, ambientais, de acesso não autorizado e danos.

4.1.9 A7.9 Segurança de ativos fora das instalações da organização

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Proteger os ativos que se encontram fora das dependências da PMS.
PROPÓSITO: Evitar perdas, danos, roubos ou comprometimento de ativos fora das dependências da organização e interrupção da operação.

4.1.10 A7.10 Mídia de armazenamento

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Gerenciaras mídias de armazenamento através do ciclo de vida de aquisição, uso, transporte e descarte de acordo com o esquema de classificação e de requisitos de manuseio.
PROPÓSITO: Garantir a divulgação, modificação, remoção ou destruição de informações contidas em mídias de armazenamento apenas de forma autorizada.

4.1.11 A7.11 Serviços de infraestrutura

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo #Detectivo	#integridade #Disponibilidade	#Proteger #Detectar	#Proteção

CONTROLE: Proteger as instalações de processamento de informações contra falas de energia e outras interrupções causadas por falhas nos serviços de infraestrutura.
PROPÓSITO: Evitar perdas, danos ou comprometimento de informações e outros ativos associados, ou a interrupção das operações da organização devido à falha e interrupção nos serviços de infraestrutura.

4.1.12 A7.12 Segurança de cabeamento

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Proteger os cabos que transportam energia, dados ou que sustentam serviços de informação contra interceptação, interferência ou danos.
PROPÓSITO: Evitar perdas, danos, roubo ou comprometimento de informações e outros ativos associados a interrupção das operações da organização ligados ao cabeamento de energia e de comunicação.

4.1.13 A7.13 Manutenção de equipamentos

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção, #Resiliência

CONTROLE: Manter o funcionamento dos equipamentos para garantira a disponibilidade, integridade e confidencialidade da informação.
PROPÓSITO: Evitar perdas, danos, roubos ou comprometimento de informações e outros ativos associados por motivo de interrupção das operações causada por falta de manutenção.

4.1.14 A7.14 Descarte seguro ou reutilização de equipamentos

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Verificar os itens dos equipamentos a serem descartados e que contenham mídia de armazenamento, para garantir que quaisquer dados confidenciais não sejam expostos. Remover os softwares licenciados com segurança antes do descarte ou reutilização.
PROPÓSITO: Evirar o vazamento de informações através do equipamento que seja descartado ou reutilizado.

5 Controles Tecnológicos

Contemplam medidas de segurança da informação implementadas por meio de ferramentas e recursos de TI. A norma NBR ISO/IEC 27.002:2022 orienta a adoção de 34 (trinta e quatro) controles organizacionais, codificados a partir da nomenclatura "A8".

5.1.1 A8.1 Dispositivos endpoint do usuário

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Proteger as informações armazenadas, processadas ou acessíveis através de dispositivos endpoint do usuário.
PROPÓSITO: Proteger informações contra os riscos introduzidos pelo uso de dispositivos endpoint do usuário nas redes da PMS.

5.1.2 A8.2 Direitos de acessos privilegiados

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Restringir e gerenciar a atribuição e o uso de direitos de acessos privilegiados.
PROPÓSITO: Assegurar que apenas usuários, componentes de software e serviços autorizados recebam direitos de acessos privilegiados.

5.1.3 A8.3 Restrição de acesso a informação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Restringir o acesso às informações e outros ativos associados de acordo com a política de tema específico sobre o controle de acesso.
PROPÓSITO: Garantir apenas o acesso autorizado e impedir o acesso não autorizado às informações e outros ativos associados.

5.1.4 A8.4 Acesso ao código fonte

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Gerenciar os acessos de leitura e escrita ao código-fonte, ferramentas de desenvolvimento e bibliotecas de software.
PROPÓSITO: Evitar a introdução de funcionalidades não autorizadas, prevenir mudanças não intencionais ou maliciosas e manter a confidencialidade de propriedade intelectual valiosa.

5.1.5 A8.5 Autenticação segura

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Implementar tecnologias e procedimentos de autenticação seguros, com base em restrições de acesso a informação e a política de tema específico de controle de acesso.
PROPÓSITO: Assegurar que um usuário ou uma entidade seja autenticada com segurança, quando são concedidos o acesso a sistemas, aplicativos e serviços.

5.1.6 A8.6 Gestão da capacidade

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo #Detectivo	#integridade #Disponibilidade	#Continuidade	#Governança, #Ecosistema,#Proteção

CONTROLE: Monitorar e ajustar o uso dos recursos de acordo com os requisitos atuais e esperados pela capacidade.
PROPÓSITO: Assegurar a capacidade necessária de instalações de processamento de informações, recursos humanos, escritórios e outros serviços de infraestrutura.

5.1.7 A8.7 Proteção contra malware

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo #Detectivo #Corretivo	#Confidencialidade #integridade #Disponibilidade	#Proteger #Detectar	#Proteção # Defesa

CONTROLE: Implementar e apoiar a proteção contra malware através da conscientização adequada ao usuário.
PROPÓSITO: Assegurar que as informações e outros ativos associados estejam protegidos contra malware.

5.1.8 A8.8 Gestão de vulnerabilidades técnicas

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar #Proteger	#Proteção #Defesa

CONTROLE: Obter informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliar e implementar medidas apropriadas para mitigá-las.
PROPÓSITO: Evitar a exploração de vulnerabilidades técnicas.

5.1.9 A8.9 Gestão de configuração

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Estabelecer configurações de segurança, de hardware, software, serviços e redes. Implementar, documentar, monitorar e revisar estas configurações regularmente.
PROPÓSITO: Assegurar que o hardware, o software, os serviços e as redes funcionem corretamente com as configurações de segurança necessárias e que estas não sejam alteradas indevidamente.

5.1.10 A8.10 Exclusão de informações

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade	#Proteger	#Proteção

CONTROLE: Excluir as informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento sejam excluídas quando não forem mais necessárias.
PROPÓSITO: Evitar a exposição desnecessária de informações confidenciais e estar em conformidade com requisitos legais, estatutários, regulatórios e contratuais para a exclusão de informações.

5.1.11 A8.11 Mascaramento de Dados

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade	#Proteger	#Proteção

CONTROLE: Utilizar o recurso de mascaramento de dados de acordo com a política de tema específico sobre controle de acesso e outros requisitos relacionados aos negócios, levando em consideração a legislação aplicável.
PROPÓSITO: limitar a exposição de dados confidenciais, incluindo informações pessoalmente identificáveis, e cumprir requisitos legais, estatutários, regulatórios e contratuais.

5.1.12 A8.12 Prevenção de vazamento de dados

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo, #Detectivo	#Confidencialidade	#Proteger, #Detectar	#Proteção, #Defesa

CONTROLE: Aplicar medidas de prevenção de vazamento de dados a sistemas, redes e quaisquer outros dispositivos que processam, armazenam ou transmitam informações confidenciais.
PROPÓSITO: Prevenir e detectar a divulgação e extração não autorizada de informações por indivíduos ou sistema.

5.1.13 A8.13 Cópia de Segurança (Backup) das informações

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Corretivo	#Integridade #Disponibilidade	#Recuperar	#Proteção

CONTROLE: Manter cópia de segurança das informações, softwares e sistemas. Testar regularmente de acordo com a política específica acordada sobre cópia das informações.
PROPÓSITO: Permitir a recuperação dos dados ou sistemas.

5.1.14 A8.14 Redundância dos recursos de tratamento das informações

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Disponibilidade	#Proteger	#Proteção,#Resiliência

CONTROLE: Implementar redundância nas instalações de processamento das informações para atender aos requisitos de disponibilidade.
PROPÓSITO: Assegurar o funcionamento contínuo das instalações de processamento de informações.

5.1.15 A8.15 Log

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Detectivo	#Confidencialidade #integridade #Disponibilidade	#Detectar	#Proteção, #Defesa

CONTROLE: Produzir registros (logs) de atividades.
PROPÓSITO: Registrar eventos, gerar evidências, assegurar a integridade das informações de registro, prevenir contra acesso não autorizado, identificar eventos de segurança da informação que possam levar a um incidente de segurança e apoiar investigações.

5.1.16 A8.16 Atividades de monitoramento

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Detectivo, #Corretivo	#Confidencialidade #integridade #Disponibilidade	#Detectar, #Responder	#Defesa

CONTROLE: Monitorar redes, sistemas e aplicativos para detectar comportamentos anômalos e ações inapropriadas.
PROPÓSITO: Avaliar e detectar possíveis incidentes de segurança da informação.

5.1.17 A8.17 Sincronização do relógio

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Detecção	#Integridade	#Proteger, #Detectar	#Proteção, #Defesa

CONTROLE: Sincronizar os relógios dos sistemas de processamento de informações.
PROPÓSITO: Permitir a correlação e análise de eventos relacionados à segurança e registro de dados. Apoiar investigações sobre coincidentes de segurança.

5.1.18 A8.18 Uso de programas utilitários privilegiados

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Controlar e restringir o uso e acesso de programas que possam ser capazes de substituir os controles de sistemas e aplicativos.
PROPÓSITO: Assegurar que os programas utilitários não sejam utilizados para prejudicar os controles dos sistemas, comprometendo a segurança.

5.1.19 A8.19 Instalação de software em sistemas operacionais

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#proteger	#Proteção

CONTROLE: Implementar procedimentos e medidas adequadas para gerenciar com segurança a instalação de software que alteram o funcionamento dos sistemas operacionais.
PROPÓSITO: Garantir a integridade dos sistemas operacionais e evitar a exploração de vulnerabilidades técnicas.

5.1.20 A8.20 Segurança de redes

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo #Detectivo	#Confidencialidade #integridade #Disponibilidade	#Proteger, #Detectar	#Proteção

CONTROLE: Proteger, gerenciar e controlar os dispositivos de rede.
PROPÓSITO: Proteger as informações nas redes e suas instalações de processamento de informações de suporte contra o comprometimento da segurança.

5.1.21 A8.21 Segurança dos serviços de rede

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: identificar, implementar e monitorar mecanismos de segurança, níveis de serviço e requisitos de rede.
PROPÓSITO: Garantir a segurança no uso de serviços de rede.

5.1.22 A8.22 Segregação de redes

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Segregar grupos de serviços, usuários. e sistemas de informação de acordo com a classificação e categoria de risco. Dividir a rede em perímetros de segurança e controlar o tráfego entre eles com base nas necessidades de negócios.
PROPÓSITO: Proteger a rede e evitar perda de dados e sistemas de informação.

5.1.23 A8.23 Filtragem da Web

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Gerenciar o acesso a sites externos.
PROPÓSITO: Reduzir a exposição a conteúdo malicioso. Proteger os sistemas de serem comprometidos por malware. Impedir o acesso a sites da web não autorizados.

5.1.24 A8.24 Uso de criptografia

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Definir e implementar regras para o uso efetivo da criptografia, incluindo o gerenciamento de chaves criptográficas.
PROPÓSITO: Assegurar o uso adequado e eficaz da criptografia para proteger a confidencialidade, autenticidade e integridade das informações.

5.1.25 A8.25 Ciclo de vida do desenvolvimento seguro

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Estabelecer e aplicar regara para o desenvolvimento seguro de software e sistemas.
PROPÓSITO: Assegurar que a segurança da informação seja projetada e implementada dentro do ciclo de vida de desenvolvimento de softwares e sistemas.

5.1.26 A8.26 Requisitos de segurança do aplicativo

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção, #Defesa

CONTROLE: Especificar e implementar requisitos de segurança da informação ao desenvolver ou adquirir aplicativos.
PROPÓSITO: Assegurar que os requisitos de segurança da informação sejam abordados ao desenvolver ou adquirir aplicativos.

5.1.27 A8.27 Princípios de seguros de arquitetura e engenharia de sistemas

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Estabelecer, aplicar, documentar e manter princípios de segurança para atividades de arquitetura e engenharia de sistemas.
PROPÓSITO: Assegurar que os sistemas de informação sejam projetados, implementados e operados com os requisitos de segurança adequados em todas as fases do ciclo de desenvolvimento.

5.1.28 A8.28 Codificação segura

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Utilizar linguagens de codificação que possuem os requisitos de segurança da informação adequados para o desenvolvimento de softwares.
PROPÓSITO: Assegurar que o software seja escrito com segurança, reduzindo o número de vulnerabilidades.

5.1.29 A8.29 Testes de segurança em desenvolvimento e aceitação

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Identificar	#Proteção

CONTROLE: Definir processos de testes de segurança no ciclo de vida do desenvolvimento de sistemas e aplicativos.
PROPÓSITO: Validar se os requisitos de segurança são atendidos quando aplicativos ou códigos são implantados no ambiente de processamento de dados.

5.1.30 A8.30 Desenvolvimento terceirizado

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo, #Detectivo	#Confidencialidade #integridade #Disponibilidade	#Identificar, #Detectar #Proteger	#Governança, #Ecosistema,#Proteção

CONTROLE: Dirigir, monitorar e analisar criticamente as atividades relacionadas à terceirização de desenvolvimento de sistemas.
PROPÓSITO: Assegurar que as medidas de segurança da informação exigidas pela organização sejam implementadas na terceirização do desenvolvimento de sistemas.

5.1.31 A8.31 Separação dos ambientes de desenvolvimento, teste e produção

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Separar e proteger os ambientes de desenvolvimento, de homologação e de produção.
PROPÓSITO: Proteger o ambiente de produção e os dados de algum comprometimento nas atividades de desenvolvimento e testes de sistemas.

5.1.32 A8.32 Gestão de mudanças

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Proteção

CONTROLE: Estabelecer mudanças e alterações de procedimentos de gestão de segurança em caso de aperfeiçoamentos ou atualizações tecnológicas.
PROPÓSITO: Preservar a segurança da informação quando ocorrerem mudanças de configuração do ambiente de processamento de informações ou atualizações tecnológicas.

5.1.33 A8.33 Informações de Teste

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade	#Proteger	#Proteção

CONTROLE: Documentar, gerenciar e manter as informações de testes realizados para atestar a segurança dos sistemas de informação.
PROPÓSITO: Assegurar a relevância e confiabilidade dos resultados dos testes realizados para atestar a segurança dos sistemas e do ambiente de processamento de informações.

5.1.34 A8.34 Proteção de sistemas de informação durante os testes de auditoria

Tipo de controle	Propriedades	Conceitos	Domínios da Segurança
#Preventivo	#Confidencialidade #integridade #Disponibilidade	#Proteger	#Governança, #Ecosistema,#Proteção

CONTROLE: Planejar e acordar atividades de auditoria envolvendo a avaliação de sistemas e ambientes de informação.

PROPÓSITO: Minimizar o impacto da auditora e outras atividades em sistemas e processos de negócio.

ANEXO IV

SALVADOR
PREFEITURA

Política de Backup e de Restauração de Arquivos Digitais da PMS

Documento de Normas Administrativas

GSI – PBR PMS
V 1.0

Política de Backup e de Restauração de Arquivos Digitais da PMS (PBR PMS)	*Versão: 1.0*
	Data: 13/11/2023
Para Divulgação	*COGEL/DITEC/GSE*

Histórico de revisões

Versão	**Data**	**Alteração**
Versão 1.0	13/11/2023	Lançamento da Primeira versão do PBR PMS

Sumário

1 Contextualização 4
2 Objetivo 4
3 Aplicação 4
4 Glossário de Termos e Definições Utilizados Neste Documento 4
5 Objetivos 5
6 Princípios 5
7 Backup 6
8 Da Frequência e Retenção dos Dados 6
9 Da Solicitação de Salvaguarda dos Dados 7
10 Do uso da rede 7
11 Do transporte e armazenamento 7
12 Dos testes de backup 8
13 Do Descarte 8
14 Restauração e Teste 8
15 Plano de Back-Up 9
15.1 Classificação da informação 9
15.2 Armazenamento 9
15.3 Documentação do backup e recuperação dos dados 9
15.4 Escolha de hardware, software e mídias 9
15.5 Definição do local dos dados a serem armazenados 9
15.6 Backup remoto: 9
15.7 Contratação de site de backup remoto 10
15.8 Transmissão dos dados para Backup Remoto 10
15.9 Transportes de mídias 10
15.10 Agendamento do backup 10
15.11 Período de retenção das mídias e guarda de mídias 10
15.12 Testes de recuperação e backup 10

1 Contextualização

Para a estratégia de backup de dados, deve-se compreender por que o motivo do backup, o que é necessário para o plano de backup, saber onde o backup deve estar, como recuperá-lo e então combinar as ferramentas para servir estas necessidades.

No sentido de assegurar sua missão, é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças.

O presente documento apresenta a Política de Backup e Restauração de Arquivos Digitais da PMS, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

2 Objetivo

A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela Companhia de Governança Eletrônica de Salvador (COGEL) e formalmente definidos como de necessária salvaguarda na Prefeitura Municipal de Salvador (PMS), para se manter a continuidade do negócio.

3 Aplicação

Esta política se aplica a todos os dados no âmbito da PMS, incluindo dados armazenados em um serviço de nuvem Pública ou Privada.

A definição de dados críticos e o escopo desta política de backup serão revisados no mínimo a cada 2 anos.

Os serviços de TI críticos da PMS devem ser formalmente elencados pela COGEL/DITEC e o Comitê Consultivo de Segurança da Informação (CCS) da PMS.

Esta política se aplica a todos que podem ser criadores e/ou usuários de tais dados na PMS. A política também se aplica a terceiros que acessam e usam na [organização] sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade da [organização]

Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).

A salvaguarda dos dados em formato digital pertencentes a serviços de TI da PMS, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

4 Glossário de Termos e Definições Utilizados Neste Documento

Alta disponibilidade - O conceito da alta disponibilidade é ter os sistemas e seus dados disponíveis vinte e quatro horas por dia, sete dias por semana, e trezentos e sessenta e cinco dias por ano. Sabe-se que obter uma disponibilidade próxima a cem por cento não é uma realidade para todas as organizações devido ao custo. O objetivo é projetar e construir sistemas altamente disponíveis minimizando as faltas ou perdas, planejadas ou não, que podem ser causadas por pontos críticos de falha. Para se ter a alta disponibilidade é necessária a redundância de recursos para tornar o backup de dados de fácil e rápida recuperação;

Backup: Cópia de um sistema completo ou de um ou mais arquivos guardados em diferentes dispositivos de armazenamento;

Backup on-line - Permite a execução do backup, mesmo com o sistema em operação. Neste período os usuários podem utilizar a aplicação e/ou a base de dados e executar ações normais, tais como a atualização e a recuperação dos dados com o sistema funcionando normalmente;

Backup off-line - Feito quando o sistema não está em operação. Os usuários não podem conectar a uma aplicação ou à base de dados e nesse período não haverá nenhuma atividade no sistema, exceto o processo de backup;

Backup completo – É o backup de todas as bases de dados e de todos os arquivos envolvidos na aplicação;

Backup incremental - É o backup dos dados que foram modificados. Esse backup somente conterá os dados modificados desde o último backup completo ou desde o último backup incremental;

Backup local - É feito no mesmo lugar em que se encontram os dados originais;

Backup remoto – É a cópia segura dos dados em local distante dos dados principais.

Custodiante da Informação - Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

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.

Disponibilidade - Período em que usuários e processos estão funcionando normalmente. A disponibilidade requer que o sistema forneça redundância para eliminar pontos críticos de falha ou Single Point Of Failure (SPOF).

Disponibilidade continua - A soma da alta disponibilidade e de operações contínuas leva à disponibilidade contínua.

Eliminação - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Gerenciamento do ciclo de vida das informações - As estratégias de Gerenciamento do Ciclo de Vida das Informações ou Information Lifecycle Management (ILM) são projetadas para melhorar a gerência de criação, o arquivamento e/ou a remoção da informação.

Janela de backup - É o período em que o backup é executado.

Mídia - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

Recovery Point Objective (RPO) – é a quantidade de dados perdida, em unidade de tempo, aceitável para ser refeita após um desastre.

Recovery Time Objective (RTO) – é quanto tempo a organização pode esperar pela recuperação de seus sistemas depois de um desastre.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.

TI: Tecnologia da Informação.

Usuário: todo funcionário, prestador de serviço, estagiário e afins que tenham acesso aos recursos tecnológicos oferecidos pela PMS.

5 Objetivos

A política de Segurança da Informação e outros controles têm a finalidade de procurar garantir que a segurança seja mantida e que os dados armazenados nos computadores sejam confiáveis e disponíveis.

De acordo com a norma NBR ISO/IEC 17799 (ABNT, 2005), é importante que as cópias de segurança, ou seja, o backup, das informações e das aplicações de software seja efetuado e testado regularmente conforme a política de geração de cópias definida.

As normas e recomendações de segurança para backup de dados pertencentes ao conjunto de política de Segurança da Informação devem ser baseadas em estratégias que visem preservar as informações importantes para os negócios da organização.

É importante fazer uma avaliação dos riscos envolvidos para decidir o que realmente precisa ser protegido e a quantidade de recursos que devem ser utilizados para a economia deles.

Justificativa:

- Proteção dos dados para a continuidade dos negócios, prevenção contra desastres e recuperação segura dos dados, para que esses estejam integrais e disponíveis;
- Atendimento a padrões de segurança e a leis e regulamentos nacionais e internacionais;
- Maior confiabilidade e crédito por parte dos clientes.

6 Princípios

a) A Política de Backup e Restauração de Dados deve estar alinhada com a Política de Segurança da Informação da PMS

b) A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional;
c) As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI;
d) As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada;
e) As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização;
f) O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica;
g) É desejável que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos;
h) A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização;
i) Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup;
j) Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

7 Backup

Os servidores são configurados para que diariamente, em horário pré-determinado, sejam realizadas as atividades de Backup de arquivos localizados no Data Center da COGEL para um Hard Drive interno e para um servidor externo ao Data Center.
Além do backup local, a PMS conta com um outro servidor para receber os arquivos de backup, como plano de contingência, armazenando os backups.
Tipos de backup:
- Completo (full);
- Incremental;
- Diferencial.

Salvo indicação em contrário, o backup dos dados do sistema será feito de acordo com a seguinte programação padrão:
- Backup incremental diário (segunda a sábado), armazenado no local;
- Backup completo semanal (sábado a domingo), armazenado externamente.

Sempre que possível, os backups devem ser iniciados às 12h da manhã de sábado para permitir mais tempo durante o fim de semana para realizar o backup e tempo suficiente para lidar com quaisquer problemas que possam surgir durante o processo.

8 Da Frequência e Retenção dos Dados

Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.
Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.
Os backups dos serviços de TI críticos da PMS devem ser realizados utilizando-se as seguintes frequências temporais: Diária; Semanal; Mensal e Anual.
Os serviços de TI críticos da PMS devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:
- I – Diária: 2 meses;
- II – Semanal: 4 meses;
- III – Mensal: 1 ano;
- IV – Anual: 5 anos.

Os serviços de TI NÃO críticos da PMS devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:
- I – Diária: 1 meses;
- II – Semanal: 2 meses;
- III – Mensal: 6 meses;
- V – Anual: 2 anos.

9 Da Solicitação de Salvaguarda dos Dados

A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelo(s) responsável(s) pelo sistema, com a anuência prévia e formal do(s) responsável(s), refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:
I. Escopo (dados digitais a serem salvaguardados);
II. Tipo de backup (completo, incremental, diferencial);
III. Frequência temporal de realização do backup (diária, semanal, mensal, anual);
IV. Prazo de Retenção;
V. RPO;
VI. RTO.

A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas a COGEL/DITEC. A aprovação para execução da alteração depende da anuência do(s) responsável(s). Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

10 Do uso da rede

O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da organização, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI.
A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.
O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável pela administração da rede de dados da COGEL/DITEC.

11 Do transporte e armazenamento

As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:
- A criticidade do dado salvaguardado;
- O tempo de retenção do dado;
- A probabilidade de necessidade de restauração;
- O tempo esperado para restauração;
- O custo de aquisição da unidade de armazenamento de backup;
- A vida útil da unidade de armazenamento de backup.

O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.
Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.
A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo 30 dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.
As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.
As fitas de backup serão transportadas e armazenadas conforme descrito:
- A mídia será claramente identificada e armazenada em uma área segura acessível apenas para pessoa(s) autorizada(s) ou o fornecedor de armazenamento seguro de mídia externo contratado usado pela PMS;
- A mídia não será deixada sem supervisão durante o transporte;
- Backups completos diários serão mantidos por 1 semana e armazenado no local em um cofre à prova de água ou fogo fisicamente protegido, localizado em uma sala fora do data center.
- Backups completos semanais serão mantidos por um período de 4 semanas, e enviado a um local de armazenamento de mídia externo fisicamente protegido. Depois de 4 semanas, as fitas serão devolvidas à TI e serão reutilizadas ou destruídas.
-

12 Dos testes de backup

Os backups serão verificados periodicamente a cada semana. Os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha
A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.
Os testes devem ser realizados em todos os backups produzidos independente do ambiente.
Os testes de restauração dos backups devem ser realizados, por amostragem uma vez por semana, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.
Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.
Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso
Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo CCS.

13 Do Descarte

Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.
A mídia de backup será retirada e descartada conforme descrito abaixo:
- A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados;
- A TI garantirá a destruição física da mídia antes do descarte.
-

14 Restauração e Teste

A restauração de dados deve ser solicitada a COGEL/DITEC e será realizada de acordo com os procedimentos específicos. A verificação e o teste de restauração, serão realizados sempre que possível por meio de um software de backup, configurado para verificar automaticamente as condições do backup.
O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:
- A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através do GLPI;
- A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup;
- A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações;
- O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

O cronograma de restauração de dados será definido levando-se em conta:
- o tempo de restauração, preferencialmente definido em Acordo de Nível de Serviço (SLA) entre as áreas de negócio e de TIC e será proporcional ao volume de dados necessários para o restore;

- Backups externos serão disponibilizados em aproximadamente em 1 dia de uma falha catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um;
- Backups externos serão disponibilizados em aproximadamente em 8 horas de uma falha não catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.
-

15 Plano de Back-Up

O Plano de Cópia e Restauração de Arquivos Digitais da PMS é o documento que deve especificar a frequência do backup, por exemplo, diário ou semanal, incremental ou completo, baseada na criticidade dos dados e na frequência em que informação nova é introduzida. Elas devem designar o local de dados armazenados, procedimentos de nomeação de arquivos, frequência de trocas das mídias, e método para transportar os dados.

15.1 Classificação da informação

Análise de riscos das informações, considerando:

- Criticidade da informação para os negócios
- Prioridade de recuperação
- Período de retenção
- Datas de criação, atualização e exclusão
- Permissões e restrições de acesso
- Reclassificação das informações

15.2 Armazenamento

Fazer o backup apenas dos dados necessários:

- Separação de arquivos, de programas e aplicações;
- Armazenar dados com nomes padronizados:
- Manter os dados armazenados apenas pelo período necessário.

15.3 Documentação do backup e recuperação dos dados

Considerar no mínimo:

- Documentação de todos os processos de backup e Recuperação de dados;
- Utilização de Padrões e ferramenta de software adequada para documentação;
- Avaliação e revisão da documentação de backup e recuperação;
- Backup da documentação.

15.4 Escolha de hardware, software e mídias

Considerar no mínimo:

- Velocidade para o backup e recuperação dos dados;
- Espaço a ser ocupado pelos dados;
- Administração e utilização simplificada;
- Período de retenção dos dados;
- Confiabilidade.

15.5 Definição do local dos dados a serem armazenados

Considerar no mínimo:

- Garantia de seguranças física e lógica;
- Controle de temperatura, umidade, prevenção contra incêndio, controles de energia elétrica etc.

15.6 Backup remoto:

- A Informação é crítica para os negócios;
- A informação precisa de contingência;
- Os dados precisam de um longo período de retenção;
- Os dados precisam ser consultados continuamente;
- Para atendimento a padrões de segurança.

15.7 Contratação de site de backup remoto

Considerar no mínimo:

- Segurança física e lógica;
- Distância geográfica:
- Acessibilidade;
- Conformidade da empresa contratada com padrões de segurança.

15.8 Transmissão dos dados para Backup Remoto

Considerar no mínimo:

- Facilidades de velocidade e segurança de conexões de rede e de Internet;
- Criptografia para os dados sigilosos.

15.9 Transportes de mídias

Considerar no mínimo:

- Confiança e comprometimento de todo o pessoal que manipula as mídias;
- Criptografia para os dados sigilosos.

15.10 Agendamento do backup

Considerar no mínimo:

- Frequência do backup de acordo com a criticidade, atualizações e outros atributos das informações;
- Tecnologias que permitam executar o backup quando o sistema está em operação

15.11 Período de retenção das mídias e guarda de mídias

Considerar no mínimo:

- Instruções de guarda e tempo de vida útil das mídias;
- Local de armazenamento das mídias.

15.12 Testes de recuperação e backup

Considerar no mínimo:

- Resultados dos testes de backup e recuperação;
- Documentação de medidas adotadas;
- Estimativa do tempo de recuperação, incluindo o tempo para identificar o problema e a solução, de acordo com tipo o armazenamento.

ANEXO V

SALVADOR
PREFEITURA

Política de Segurança da Informação

Plano de Continuidade de Negócios de TI

PCNTI PMS - COGEL
V 1.0

Histórico de revisões

Versão	**Data**	**Alteração**
Versão 1.0	10/11/2023	Lançamento da Primeira versão adequada a PSI PMS

Sumário

1 Introdução 4
2 Objetivo 4
3 Glossário de Termos e Definições Utilizados neste Documento 4
4 Metodologia 5
4.1 Plano de Gestão de Riscos e de Análise de Impacto (PGRAI) 5
4.2 Plano de Contingência de TI (PCTI) 5
4.3 Plano de Continuidade Operacional (PCO) 5
4.4 Plano de Administração de Crises (PAC) 5
4.5 Plano de Recuperação de Desastres (PRD) 5
5 Aplicabilidade 5
6 Papéis e Responsabilidades 6
6.1 Dos Usuários 6
6.2 Dos Núcleos de TI da PMS 6
6.3 Do Comitê Consultivo de Segurança (CCS) 6
6.4 Da Assessoria Jurídica da PMS 6
6.5 Gerência de Infraestrutura 6
6.6 Gerência de Suporte 7
6.7 Gerência de Segurança da Informação 7
7 Referências Legais e de Boas Práticas 7
8 Plano de Gestão de Riscos e de Análise de Impacto 8
9 Plano de Contingência de TI (PCTI) 9
9.1 Destinatários 9
9.2 Classificação por Níveis de Incidentes 9
9.3 Problemas com Computadores e Equipamentos de TI 10
9.4 Problemas de Conexão com a rede Interna 10
9.5 Problemas de Conexão com a Internet 10
9.6 Problemas com Acesso aos Sistemas Corporativos Internos 10
9.7 Problemas com Equipamentos de Rede 10
9.8 Problemas Físicos com Cabeamento da Rede Interna 10
9.9 Problemas com Falta de Energia 11
9.10 Ataques Internos 11
9.11 Ataques cibernéticos 11
9.12 Outros Problemas 12
9.13 Quem deve comunicar 12
9.14 A quem comunicar 12
9.15 Como comunicar 12
10 Plano de Continuidade Operacional (PCO) 12
10.1 Objetivo e Escopo 13
10.2 Atividades 13
10.3 Recursos 13
10.4 Encerramento do PCO 13
11 Plano de Administração de Crises (PAC) 13
11.1 Objetivo e Escopo 13
11.2 Atividades 13
11.3 Encerramento do PAC 14
12 Plano de Recuperação de Desastres (PRD) 14
12.1 Objetivo e Escopo 14
12.2 Atividades 15
12.3 Encerramento do PRD 15

1 Introdução

Uma vez que falhas nos serviços de Tecnologia da Informação e Comunicação (TIC) impactam diretamente a continuidade da prestação dos serviços dentro da Prefeitura Municipal de Salvador (PMS), este plano provê medidas de proteção rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais em casos de incidentes graves ou desastres a partir da especificação das ameaças e riscos identificáveis na organização e análise de seus impactos, caso essas ameaças se concretizem.

2 Objetivo

O Plano de continuidade dos Negócios da Prefeitura Municipal de Salvador (PCN PMS) tem por objetivo assegurar a continuidade dos serviços em caso de algum evento que interrompa a operação de um ou mais processos de negócio.

O foco está em garantir a continuidade dos processos e informações cruciais para a sobrevivência da organização, no menor tempo possível, com o objetivo de minimizar os efeitos resultantes de um desastre.

O PCNTI PMS é um processo, cujo planejamento tem como objetivo assegurar que uma organização resista a um desastre ou qualquer atividade imprevista que provoque danos aos ativos críticos, pondo em risco qualquer processo de negócio. De acordo com a norma NIST SP 800-34, o plano pode ser elaborado englobando somente os processos críticos do negócio ou pode compor todos os processos de uma organização.

3 Glossário de Termos e Definições Utilizados neste Documento

Ameaça: causa potencial de um incidente indesejado que pode resultar em dano para a organização.

Áreas Sensíveis: Áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências da emergência. Dentre elas encontram-se os laboratórios de informática, salas administrativas, Data Center e demais locais que possuam equipamentos de informática;

Área Vulnerável: Área atingida pela extensão dos efeitos provocados por um evento de falha;

Ativo: qualquer recurso que tenha valor para a organização e cujo risco precisa ser controlado;

Contexto Externo: é o ambiente externo no qual a organização se situa e busca atingir seus objetivos (ambiente cultural, financeiro, regulatório, econômico, entre outros);

Contexto Interno: é o ambiente interno no qual a organização busca atingir seus objetivos (governança, estrutura organizacional, políticas, normas, objetivos, diretrizes, cultura organizacional, entre outros);

Contingência: Situação de risco com potencial de ocorrer, inerente as atividades, serviços e equipamentos, e que ocorrendo se transformará em uma emergência;

Emergência: Situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos aos próprios sistemas ou equipamentos ou ao desempenho do trabalho dos usuários;

Evento de Segurança da Informação: ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

Firewall: É uma solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas;

GLPI (Gestão Livre de Parque de Informática): Sistema de abertura de chamados técnicos;

Impacto: uma das consequências da ocorrência de um evento. Ocasiona mudança adversa no nível obtido dos objetivos;

Incidente: É um evento inesperado ou situação que altera a ordem normal das coisas, capaz de causar danos aos sistemas e aos equipamentos de TI;

Intervenção: É a atividade de atuar durante a emergência, seguindo planos de ações para corrigir ou minimizar os possíveis danos aos equipamentos e sistemas de TI;

Parceiros: Empresas, órgãos públicos e demais instituições que possuem contrato com a PMS com objetivos em comum, unindo esforços em suas competências e expertises, sem que haja remuneração, mas apenas empenho de serviços por cada parte;

Probabilidade do Risco: possibilidade de concretização de uma ameaça;
Nível de Risco: magnitude do risco, expressa em termos da combinação das consequências e de suas probabilidades;
Risco: Diz respeito a uma eventualidade, possibilidade de ocorrer;
Risco Residual: Risco remanescente após o tratamento de risco ter sido implementado. Pode conter riscos não identificados;
Risco de Segurança da Informação: possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos. É medido em função da combinação da probabilidade de um evento e de sua consequência;
Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
VM: Máquina Virtual, virtualizada no servidor;
Zabbix: Ferramenta que pode ser utilizada para monitoramento da infraestrutura de rede e sistemas e aplicações.

4 Metodologia

A metodologia a ser adotada neste PCNTI PMS pressupõe a administração de planos específicos que são contidos neste documento:

4.1 Plano de Gestão de Riscos e de Análise de Impacto (PGRAI)

Tem por objetivo avaliar o nível de risco dos incidentes de Segurança da informação.

4.2 Plano de Contingência de TI (PCTI)

As Ações deste plano têm como objetivo evitar que falhas nos serviços de Tecnologia da Informação (TI) tragam impacto diretamente em todos os órgãos da PMS. Pretende-se com este plano definir procedimentos, ações e medidas rápidas para os processos críticos de TI.

4.3 Plano de Continuidade Operacional (PCO)

Objetiva garantir a continuidade dos serviços essenciais de TI críticos na ocorrência de desastres, enquanto recupera-se o ambiente principal.

4.4 Plano de Administração de Crises (PAC)

Tem por objetivo definir as atividades das equipes envolvidas e orquestrar as ações de contingência e comunicação durante e após a ocorrência de um desastre, com intuito de minimizar impactos até a superação da crise.

4.5 Plano de Recuperação de Desastres (PRD)

Tem por objetivo orientar procedimentos para que, uma vez controlada a contingência e passada a crise, a TI do DATACENTER da COGEL retome seus níveis originais de operação no ambiente principal.

5 Aplicabilidade

O PCNTI PMS será acionado quando da ocorrência de algum dos cenários de desastres, a insurgência ou ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada.
O plano também poderá ser invocado em casos de testes ou por determinação do Comitê Consultivo de Segurança da Informação (CCS) em conjunto com a alta governança da COGEL.
Este plano envolve quatro grupos:

- Contingência de Infraestruturas Físicas, assim compreendidas as situações de catástrofes naturais ou não, tais como inundações, incêndios, desabamentos, entre outros. Ocorrências que impeçam o acesso e/ou utilização das instalações do DATACENTER da COGEL, como também danos físicos relevantes a instalações e/ou equipamentos, intencionais ou não, incluindo falhas no fornecimento de energia elétrica;
- Contingência de Pessoas onde os colaboradores não estão presentes por motivos de greves, doença, licenças etc.;
- Contingência de Infraestruturas Tecnológicas compreendidas as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como hardware, software, telecomunicações, rede e segurança;
- Contingência de Serviços Externos compreendidas as situações de não prestação de serviço contratado considerado crítico aos processos da PMS.

6 Papéis e Responsabilidades

6.1 Dos Usuários

Informar o NTI ou Setor de TI de seu órgão, caso detectem algum tipo de emergência ou hipótese acidental que ocorram em alguma das áreas sensíveis da PMS.

6.2 Dos Núcleos de TI da PMS

Mitigar os impactos que porventura venham a ocorrer decorrentes de emergências que afetem os sistemas, equipamentos ou infraestrutura de TI da sua área de responsabilidade.
Entrar em contato com a instância superior de TI no caso de precisar de auxílio ou para reportar o incidente.

6.3 Do Comitê Consultivo de Segurança (CCS)

O Comitê Consultivo de Segurança (CCS) é uma estrutura matricial multidisciplinar que conta com a participação de gestores de diversas áreas da PMS. É formado por representantes das principais instâncias da instituição, incluindo a GSE.
O Comitê Consultivo se reúne semestralmente para tratar de assuntos relacionados com a segurança da informação. Reuniões adicionais podem ser realizadas sempre que for necessário para deliberar sobre alguma decisão relevante para a PMS.
É facultado ao CCS convocar ou consultar especialistas para tratar de algum assunto específico da área de Segurança da Informação no caso de algum incidente que coloque em risco a continuidade dos negócios de TI.

6.4 Da Assessoria Jurídica da PMS

A PMS deve contar com apoio jurídico da Assessoria Jurídica para aconselhamento em questões que envolvam questões legislativas, regulatórias, litigiosas ou em questões que envolvam matéria específico do direito Digital, em caso de interrupção de serviços de TI que tragam danos ou prejuízos à atividade da PMS.

6.5 Gerência de Infraestrutura

Responsável pelas instalações físicas que abrigam sistemas de TI e pela garantia que as instalações alternativas serão mantidas adequadamente. Avalia os danos e supervisiona os reparos para o local principal no caso de a localização primária sofrer destruição ou danos. O Gerente desta equipe administrará e manterá o Plano de Administração de Crise e de Recuperação de Desastre.
Principais atividades:

- Avaliar os danos específicos de qualquer infraestrutura de rede para fornecer dados e conectividade de rede de voz, incluindo WAN, LAN e quaisquer conexões internamente dentro do DATACENTER da PMS ou de infraestrutura externa junto aos prestadores de serviço.
- Fornecer a infraestrutura de servidor físico e virtuais necessária para que a PMS execute suas operações e processos essenciais durante um desastre.
- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre. Assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes conforme necessário.
- Analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.
- Atuar como responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, se necessário.

6.6 Gerência de Suporte

Responsável por fornecer aos funcionários as ferramentas de que necessitam para desempenhar as seguintes funções da forma mais rápida e eficiente possível:

- Provisionar os funcionários da COGEL envolvidos na solução de contingência e os que trabalham remotamente com as ferramentas específicas.
- Atender aos usuários em caso necessário para realizar os testes de conectividade e de desempenho das estações de trabalho.
- Reportar à Gerência de Segurança e aos usuários de forma geral sobre atualizações de versão, modificações ou melhorias nos sistemas;
- Promover a recuperação de sistemas.

6.7 Gerência de Segurança da Informação

Responsável por prover mecanismos de segurança no ambiente principal e alternativo afim de resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, em conformidade com a Política de segurança (PSI). Deverá realizar as seguintes ações:

- Comunicar ao Comitê Consultivo de Segurança da Informação (CCS) os incidentes previstos no Plano de Gerenciamento de Incidentes;
- Avaliar o Plano de Gerenciamento de Vulnerabilidades e o Plano de Gerenciamento de Incidentes periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres;
- Facilitar e coordenar as atividades de tratamento e resposta a incidentes de Segurança da Informação;
- Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de Segurança da Informação e avaliando condições de segurança por meio de verificações de conformidade;
- Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis.
- Receber, filtrar, classificar e responder às solicitações e alertas e realizar análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências;
- Avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação;
- Emitir alertas sobre vulnerabilidades e outras notificações relacionadas à Segurança da Informação;
- Avaliar o uso de ferramentas de Segurança da Informação e Comunicação.

7 Referências Legais e de Boas Práticas

No PRD PMS foram utilizadas as seguintes referências legais e de boas práticas:

- ABNT NBR ISO 31000 (2018): estabelece princípios e orientações genéricas sobre gestão de riscos;
- ABNT NBR ISO/IEC 22301 (2020): está relacionada a gestão da continuidade de negócios e é relevante a todos os modelos e tamanhos de organizações que tem como objetivo estabelecer, implementar, manter e melhorar o sistema de informação;
- ABNT NBR ISO/IEC 27002 (2022): estabelece um guia prático para desenvolver os procedimentos necessários de segurança da informação e práticas de gestão da segurança da informação;
- NIST SP 800-30 (2012): oferece orientações para a realização de avaliação de riscos dos sistemas de informação e organizações;
- NIST SP 800-37 (2018): apresenta diretrizes para execução do quadro de gestão de riscos para sistemas de informação com o objetivo de prover instruções para a realização das atividades de categorização, seleção, controle, implementação, avaliação, autorização e monitoramento dos controles de segurança.
- Plano de Recuperação de Desastres com Foco no ERP – João José Furtado Neto e Mehan Misaghi, Centro Universitário UNISOCIESC –
- Universidade Federal do Mato Grosso do Sul - Hospital Universitário Maria Aparecida - PEDROSSIAN

8 Plano de Gestão de Riscos e de Análise de Impacto

Para identificar as necessidades da organização em relação aos requisitos de segurança da informação, é necessária uma abordagem sistemática de gestão de riscos de segurança da informação (ABNT NBR ISO/IEC 27005, 2019). O Risco de Segurança da Informação, conforme Sêmola[1], pode ser calculado pela fórmula da Figura1.

$$R = \frac{V \times A \times I}{M}$$

RISCO — VULNERABILIDADES — AMEAÇAS — IMPACTOS — MEDIDAS DE SEGURANÇA

Figura 1 - Cálculo do Risco

O risco é a hipótese de que as ameaças explorem as vulnerabilidades, causando impactos aos negócios. Esses impactos podem ser limitados por medidas de segurança, responsável pela proteção dos ativos, impedindo ou dificultando que as ameaças explorem as vulnerabilidades, diminuindo, assim, o risco.

De acordo com a ABNT NBR ISO/IEC 27005 (2019), a gestão de riscos é composta por sete etapas, conforme ilustra a Figura 2.

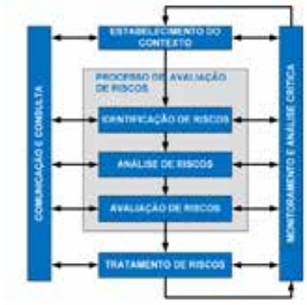

Figura 2 - Gestão de riscos.

Os critérios de riscos são parâmetros estabelecidos para avaliar a magnitude dos riscos, a fim de seja possível quantificar o impacto negativo na missão institucional da PMS.

Para efeito deste processo, definiu-se como metodologia para a análise de risco a forma proposta pela norma ABNT NBR ISO 31000:2009, a qual define o nível do risco em termos da combinação dos impactos e de suas probabilidades.

Serão utilizadas escalas quantitativas para estimar a Probabilidade e o Impacto. Tais escalas encontram-se representadas nas Tabela 1 e Tabela 2.

Peso	Critério	Probabilidade
5	Muito Alta	50% < Probabilidade <= 100%
4	Alta	20% < Probabilidade <= 50%
3	Média	8% < Probabilidade <= 20%
2	Baixa	2% < Probabilidade <= 8%
1	Muito Baixa	0% < Probabilidade <= 2%

Tabela 1 - Análise da Probabilidade

Peso	Impacto	Descrição
5	Catastrófico	Impacto máximo nos objetivos do processo avaliado, sem possibilidade de recuperação.

[1] SÊMOLA, M. Gestão da Segurança da Informação: uma visão executiva. Rio de Janeiro, RJ: Elsevier, 2014.

4	Muito Relevante	Impacto significante nos objetivos do processo avaliado, com possibilidade remota de recuperação.
3	Relevante	Impacto mediano nos objetivos do processo avaliado, com possibilidade de recuperação.
2	Pouco Relevante	Impacto mínimo aos objetivos do processo avaliado. São facilmente remediáveis.
1	Insignificante	Impacto insignificante nos objetivos do processo avaliado. Dispensa qualquer medida de reparação.

Tabela 2 - Análise do Impacto

O nível do risco é calculado pelo produto entre a probabilidade e o impacto. A Tabela 3 apresenta a Matriz de Risco, ferramenta utilizada para a classificação dos níveis de risco.

Extremo						
Elevado		PROBABILIDADE				
Médio		Muito baixa (1)	Baixa (2)	Média (3)	Alta (4)	Muito Alta (5)
Baixo						
IMPACTO	Catastrófico (5)	5	10	15	20	25
	Muito relevante (4)	4	8	12	16	30
	Relevante (3)	3	6	9	12	15
	Pouco relevante (2)	2	4	6	8	10
	Insignificante (1)	1	2	3	4	5

Tabela 3 – Matriz de Risco

9 Plano de Contingência de TI (PCTI)

O Plano de Contingência de TI da PMS (PCTI PMS) é composto por um conjunto de ações que suportem o gerenciamento de situações de contingência provocada por incidentes causadores de interrupção no andamento normal de suas atividades, garantindo as condições mínimas necessárias para a continuidade e normalização delas.

9.1 Destinatários

O presente PCTI PMS se destina a todos os administradores de serviços e sistemas de Tecnologia da Informação da PMS. Este plano deve ser seguido para garantir os serviços essenciais em caso de emergências que possam ocorrer durante as atividades de TI na PMS, visando aplicar as ações necessárias para correção e/ou eliminação do problema.

Os usuários devem ser informados deste documento e de suas atualizações e observarem as diretrizes nele estabelecidas. Elas devem estar disponíveis em documento interno de fácil e sem restrições de acesso. Em caso de dúvidas, os usuários devem buscar orientação no Setor ou Núcleo de Tecnologia da Informação (NTI).

As Recomendações de Medidas Preventivas estão diretamente relacionadas às providências para mitigação de risco na ocorrência de algum incidente.

9.2 Classificação por Níveis de Incidentes

Nível I: Hipótese acidental que pode ser controlada pela equipe de TI do órgão e que não afeta o andamento do trabalho do servidor.

Nível II: Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo servidor.

Nível III: Hipótese acidental que impede o uso de sistemas ou equipamentos de todo o órgão, impedindo assim o desenvolvimento do trabalho de todos os servidores da PMS.

Nível IV: Hipótese acidental que impede o uso de sistemas para o órgão e os seus clientes afetando não só a equipe interna como também a população.

Nível V: Hipótese acidental que impede o uso de sistemas para toda a PMS. Todo o trabalho da PMS é suspenso.

9.3 Problemas com Computadores e Equipamentos de TI

Falha que necessite reposição de peça ou reparo cuja aquisição dependa de processo licitatório.

As máquinas instaladas nos órgãos possuem contrato de manutenção ou contratos de garantia, para passar por manutenções corretivas. São feitas imagens com atualizações do sistema e softwares solicitados pelas áreas.

Os usuários, que estão utilizando os equipamentos, informam o problema ao NTI ou Setor de TI responsável por sua área através do Sistema GLPI . O Sistema envia um e-mail para o NTI alertando para um novo chamado, o qual é atribuído a um técnico que ficará responsável pelo atendimento. Caso o problema impeça o andamento dos serviços, o NTI ou Setor de TI vai até o local fazer uma primeira verificação do problema e tenta solucioná-lo no local. Caso não seja possível a resolução imediata do problema, O usuário é encaminhado a outa estação de trabalho que não esteja sendo utilizada, em uma eventual falta de estações livres a TI providenciara uma máquina backup em caráter emergencial para continuidade dos trabalhos. Após o atendimento, o solicitante é informado da conclusão/resolução do problema.

9.4 Problemas de Conexão com a rede Interna

Rompimento de cabos decorrente de execuções de obras internas, desastres ou acidentes.

O Setor de TI identificará por meio de um sistema de monitoramento (Zabbix), que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos e em qual local está ocorrendo o problema. Caso o problema de conexão seja em todo o órgão, deve-se verificar se os servidores de endereços DHCP (protocolo de configuração dinâmica de host) e de autenticação estão funcionando adequadamente. Informar a previsão do conserto ou solução aos demais servidores.

9.5 Problemas de Conexão com a Internet

O Setor de TI identificará por meio de um sistema de monitoramento do Firewall que irá comutar automaticamente para o Link Backup e pelo (Zabbix), ambos emitirão alertas com a descrição do incidente, os dispositivos envolvidos e em qual local está ocorrendo o problema. Deve-se verificar se o Firewall comutou automaticamente para o Link de Backup. Detectado problema externo de internet, abrir um chamado de suporte com a operadora, visando o reestabelecimento do serviço. Informar a previsão do conserto ou solução aos usuários envolvendo.

9.6 Problemas com Acesso aos Sistemas Corporativos Internos

O Setor de TI identificará por meio de um sistema de monitoramento (Zabbix), que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos e em qual local está ocorrendo o problema. Verificar com o órgão responsável pelo sistema se ele está em operação. Este deverá verificar as conexões de rede. Caso não esteja em execução, iniciá-lo no servidor e testar seu acesso novamente. Caso seja necessário reinicializar o servidor ou restaurar o sistema de backup para a recuperação da máquina ou arquivos, informar a previsão do conserto ou solução aos demais órgãos.

9.7 Problemas com Equipamentos de Rede

O Setor de TI identificará por meio de um sistema de monitoramento (Zabbix), que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos e em qual local está ocorrendo o problema. Caso possível, realizar a manutenção dele. Caso necessite uma intervenção mais especializada, realizar a troca do equipamento de forma que haja o menor transtorno possível no desempenho das atividades.

9.8 Problemas Físicos com Cabeamento da Rede Interna

O NTI ou Setor de TI identificará por meio de um sistema de monitoramento (Zabbix), que emitirá um alerta com a descrição do incidente, os dispositivos

envolvidos e em qual local está ocorrendo o problema. Este deverá detectar a causa do problema por meio de testes no cabeamento. Caso seja detectado um problema de cabeamento de rede, refazer a conexões. Após, verificar as demais ligações caso seja em um rack com switch e testá-lo. Caso haja necessidade, agendar ou efetuar a troca do(s) cabo(s) que estão apresentando falhas. Caso seja detectado problema de cabeamento de fibra, contingenciar com cabeamento de rede UTP e solicitar manutenção em caráter emergencial a COGEL/DITEC.

9.9 Problemas com Falta de Energia
Causada por fator externo à rede elétrica do prédio ou de sua localidade. Causada por algum fator interno ou externo que comprometa a rede elétrica do prédio como falta de fornecimento de energia, curto-circuito ou incêndio.
Caso seja identificada queda ou falta total de energia elétrica, informar a Coordenadoria Administrativa (CAD) para as devidas providências que irá verificar se a queda foi interna ou externa e solicitar as providências para o seu restabelecimento.

9.10 Ataques Internos
Ataques internos, em que os criminosos utilizam táticas para acessar de forma legítima o ambiente protegido. Ataque aos ativos do Data Center e equipamentos de TI dos órgãos vindos de dentro da PMS.
Todo usuário deve registrar incidentes de Segurança da Informação. O NTI ou setor responsável deve registrar um incidente de Segurança da Informação para o ataque interno identificado. As informações referentes aos responsáveis pelo registro de incidentes de Segurança da Informação são sigilosas, entretanto esta identificação é obrigatória.
O Gestor máximo do órgão deve ser informado e deverá encaminhar para análise de instalação de processo administrativo.
A área de Tecnologia da Informação do órgão ou entidade deve avaliar os danos ocorridos e comunicar a COGEL/DITEC para que sejam elaborados planos de ação para tratamento do incidente. O NTI ou setor de TI deverá monitorar a implementação do plano de ação estabelecido.
É vedado ao usuário intervir no tratamento dos incidentes sem a devida autorização ou qualificação.
Principais tipos de ataques internos:
Engenharia social: Explora a vulnerabilidade através do próprio usuário. Consiste em enganar as pessoas, para que elas concedam acesso sem perceberem. Entre as práticas de engenharia social estão o envio de e-mails falsos, o Phishing ou, até mesmo, o acesso físico ao dispositivo que o colaborador utiliza para trabalhar.
Sabotagem: Realizada por membros internos da organização, explora a omissão de informações ou o envio incompleto de forma proposital, a disseminação de pistas falsas ou inserção proposital de dados falsos nos sistemas. Podem ser ocasionadas por fatores como insatisfação no trabalho, alto nível de competitividade interna, rejeição a mudanças, ocorrência de fraudes e/ou tentativas de colocar interesses pessoais acima da instituição.

9.11 Ataques cibernéticos
Ataques externos que utilizam brechas em aplicações e dispositivos para acessar áreas restritas com força bruta. Ataque virtual que comprometa o desempenho, acesso aos dados ou configuração dos serviços essenciais.
Ferramentas de monitoramento do ambiente de rede da PMS detectam vulnerabilidades e incidentes envolvendo ataques cibernéticos que são analisados pela equipe de segurança da COGEL/DITEC que são tratados e analisados como incidentes de segurança da informação. A análise consiste em identificar o ataque, sua natureza e classificação, descobrir a forma de sua operação e implementar medidas corretivas e preventivas para mitigação dos riscos envolvidos.
Além disso, todo usuário deve registrar incidentes de Segurança da Informação. O NTI ou setor responsável deve registrar um incidente de Segurança da Informação para o ataque cibernético identificado e encaminhar a COGEL/DITEC para que sejam elaborados planos de ação para tratamento do incidente. O NTI ou setor de TI deverá monitorar a implementação do plano de ação estabelecido.
É vedado ao usuário intervir no tratamento dos incidentes sem a devida autorização ou qualificação.
Principais tipos de ataques cibernéticos:
Phishing: trata-se de uma corruptela da palavra pescaria, em inglês. É a prática de utilizar iscas digitais para enganar usuários, fazendo com que eles forneçam dados legítimos de acesso a um sistema sem perceberem. Um exemplo muito comum disso é a construção de sites clonados, que imitam exatamente a página de login em sistemas empresariais, bancários etc. Utilizando variações imperceptíveis na URL, eles levam o usuário a acreditar que está no endereço legítimo e digitar credenciais de login, que são registradas pelo criminoso. Assim, é possível utilizar os mesmos dados para acessar informações sensíveis com facilidade.
Malware: Também conhecido como software malicioso, é qualquer tipo de código furtivo instalado em um dispositivo (computador, smartphone, entre outros) que passa a executar ações localmente sem o conhecimento do usuário. Geralmente, eles são instalados não intencionalmente, disfarçados de outros arquivos ou embutidos em aplicações de terceiros. A partir do momento em que são ativados, agem automaticamente, realizando funções diversas. Os malwares podem ser utilizados para espionar uso de sistemas, interceptar comunicações, registrar teclas digitadas, captar e enviar dados ou até diminuir a capacidade de processamento da máquina.
Ransomware: é a categoria de malware que mais se popularizou nos últimos anos. Esse código bastante especializado tem como função criptografar dados a que tem acesso a partir do dispositivo em que foi instalado — que pode ir do disco local da máquina até bancos na nuvem. O objetivo é impedir o usa da empresa de suas próprias informações e também de dados de clientes, algo que inviabiliza a produtividade na era digital e pode acarretar vazamentos sérios. Quando bem-sucedido, o criminoso pede um resgate em dinheiro para devolver o acesso aos dados.
DDoS: o ataque de negação de serviço (DDoS) é considerada uma prática de força bruta. No modelo, o criminoso utiliza um grande número de dispositivos cooptados por malware para fazer um volume de acesso superior ao que o servidor da empresa aguenta. Quando isso acontece, o sistema sai do ar e isso se torna uma brecha para invasões ou o comprometimento de produtos digitais oferecidos pelo negócio.

9.12 Outros Problemas
Para qualquer outro tipo de problema que envolva a TI e que não seja resolvido pelo NTI ou Setor de TI, este deverá informar o problema a COGEL/DITEC através do Sistema de Suporte GLPI.

9.13 Quem deve comunicar
Qualquer usuário que detecte qualquer tipo de problema ou anomalia, referente aos sistemas, equipamentos e/ou infraestrutura de TI.

9.14 A quem comunicar
A comunicação deve ser feita para o NTI ou o Setor de TI do órgão de sua responsabilidade. Por sua vez, o NTI deverá apurar o fato ocorrido e comunicar o incidente a COGEL/DITEC para análise e resolução do incidente, quando o mesmo não puder ser resolvido em sua instância.

9.15 Como comunicar
Através do Sistema de Suporte GLPI. Em casos urgentes ou na indisponibilidade deste sistema, contactar a chefia imediata ou o NTI pessoalmente ou por telefone.

10 Plano de Continuidade Operacional (PCO)
Este Plano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais. A Gerência de Segurança (GES) é a responsável por implementar, manter e melhorar o PCO e toda a documentação inerente.

10.1 Objetivo e Escopo

É escopo deste plano garantir ações de continuidade durante e depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas das ações de contingência definidas na estratégia. São objetivos do PCO:

a) Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações de TI, mesmo após a ocorrência de um desastre, dos sistemas essenciais;
b) Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre;
c) Estabelecer uma equipe para cada plano PCO, PAC e PRD;
d) Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

10.2 Atividades

- Avaliar situação de desastre;
- Identificar ativos afetados;
- Estimar impacto de perda de dados;
- Mapear ativos a serem recuperados;
- Levantar dados de backup para restauração;
- Implantar procedimentos de recuperação;
- Testar procedimentos realizados;
- Repassar eventuais informações para demais colaboradores.

10.3 Recursos

Durante um incidente, os recursos humanos e materiais necessários para continuidade operacional devem ser relacionados de forma a refletir a necessidade de acordo com a gravidade do evento.

10.4 Encerramento do PCO

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter deverá ser emitido um parecer ao comitê relatando as atividades realizadas neste PCO. A equipe responsável pelo retorno deve emitir um parecer, relatando as atividades realizadas, para então fornecer os dados necessários para um comunicado de retorno das atividades à instituição.

11 Plano de Administração de Crises (PAC)

Este plano de Administração de Crises (PAC) especifica as ações ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos, inerente ao relacionamento entre os agentes envolvidos e/ou afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz.

11.1 Objetivo e Escopo

O objetivo deste plano é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de uma catástrofe. Já a abrangência (Escopo), é focada nas equipes (Recursos Humanos) e leva em conta os fatores históricos. Também considera os fatos que estão ocorrendo e por fim as ações futuras, que são delimitadas somente após a ocorrência de um evento. São objetivos específicos do PAC:

- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise;
- Orientar os usuários e colaboradores de forma geral, incluindo terceirizados, com informações e procedimentos de conduta;
- Informar ao Comitê Consultivo de Segurança (CCS) em tempo e com esclarecimentos condizentes com o ocorrido.
-

11.2 Atividades

A gestão de crises na área de TIC deverá ser executada conforme o tipo da crise, seguindo uma linha geral de procedimentos listados:

- Equipes de Infraestrutura e Sistemas devem avaliar a extensão do que foi afetado;
- A COGEL/DITEC deve ser informada para buscar soluções para a gestão da crise;
- Gerentes devem ser informados e consultados;
- O Comitê Consultivo de Segurança (CCS) monta um centro de gerenciamento de crises;
- A COGEL/DITEC mantém a comunicação entre equipe interna e terceiros;
- Após a recuperação, a COGEL/DITEC informa ao CCS;
- É feito o registro de informações para subsidiar a gestão de crises futuras.
-

11.3 Encerramento do PAC

O PAC será encerrado assim que o funcionamento de sistemas essenciais do Container estiver normalizado. A equipe responsável pelo retorno deve emitir um parecer relatando as atividades realizadas para o chefe do SGPTI, que por sua vez deve informar do retorno das atividades à instituição.

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do DATACENTER, a COGEL/DITEC entrará em contato com o CCS informando o retorno das operações com as informações de status dos serviços essenciais.

A GES deverá compor relatório com relação das atividades necessárias após a ocorrência dos desastres como o remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

12 Plano de Recuperação de Desastres (PRD)

Este Plano de Recuperação de Desastres (PRD) trata das ações previamente definidos para cenários de desastres, ou seja, conjunto de procedimentos para garantir que as atividades críticas retornem à operação dentro do prazo preestabelecido após a ocorrência de um desastre.

A norma NIST SP 800-37 (2018), descreve o PRD como um plano de informação do sistema com foco projetado para restaurar a funcionalidade do sistema, aplicação ou infraestrutura de instalação de computadores em um site alternativo após uma emergência, e complementa informando que se aplica a grandes rupturas, geralmente físicas, para os serviços que negam o acesso a infraestrutura de instalação principal para um período prolongado.

O PRD PMS é um plano de ação, que tem como principal objetivo restaurar, no menor tempo possível e mesmo com desempenho reduzido, os serviços de TI que sustentam os processos críticos do negócio.

O plano é acionado após o acontecimento de um desastre, podendo ser:

- voluntário (hackers, incendiários etc.);
- involuntário (acidentes, falta de energia etc.); ou
- natural (enchentes, incêndios naturais etc.).

Conforme a norma NIST SP 800-34, a estratégia de recuperação é desenvolvida através da análise dos resultados obtidos da avaliação de riscos e fornece direção na maneira com que a estratégia de continuidade possa ser executada (NIST SP 800-34, 2010).

As estratégias mais satisfatórias são aquelas que tem a melhor relação custo X benefício, são as que reduzem os riscos e exposições e que também atendem às exigências do negócio e não só de TI. Independente da estratégia escolhida, o objetivo final deve ser o mesmo, garantir uma recuperação eficiente dos processos de negócio da empresa de acordo com a análise obtida na gestão de riscos e seu tipo de negócio.

12.1 Objetivo e Escopo

Este documento determina o plano para que, uma vez controlada a contingência e passada a crise, a organização retorne aos seus níveis normais de operação. Além de avaliar possíveis vulnerabilidades dos componentes que suportam os processos de negócios críticos ao se deparar com eventos. Cabe executar um mapeamento e planejamento de sua recuperação ou restauração, sempre considerando as necessidades da PMS.

No PRD devem ser detalhados os planos de ações relativos a sites alternativos, visando à continuidade dos negócios da organização. O escopo deste documento se restringe a última etapa da recuperação de desastres. Visa garantir o retorno

a normalidade das operações e não mais sua recorrência no caso de riscos controláveis.

12.2 Atividades
Algumas atividades são essenciais durante o processo de recuperação de um desastre, sendo elas listadas nos tópicos abaixo.

- **Identificar ativos danificados** - Deverão ser identificados e listados todos os ativos danificados da ocorrência do desastre.
- **Identificar acessos interrompidos** - Deverão ser identificadas as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, rede WAN ou com o provedor de serviços.
- **Listar Serviços Descontinuados** – Deverão ser mapeados quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento da COGEL/DITEC. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storage, routers e switches, bem como respectivas configurações de firewall, DNS, rotas, vlans etc.
- **Elaborar Cronograma de Recuperação** - Após o mapeamento das perdas e impactos, deverá ser elaborado um cronograma de recuperação das aplicações levando em consideração, a priorização dos serviços essenciais, ou de acordo com determinação de nível institucional, o retorno definido para cada serviço essencial e a força de trabalho disponível.
- **Substituição de ativos e equipamentos** - Em caso de perda de ativos, deverá ser imediatamente informado a COGEL/DITEC, a necessidade de aquisição de ativos perdidos que não puderam ser recuperados. Verificar se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição. Devem ser verificados quais ativos foram danificados estão cobertos por garantia e se poderá ser acionada neste caso através da lista de fornecedores. As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC.
- **Reconfiguração de ativos e equipamentos** - A equipe de INFRAESTRUTURA deverá verificar que as configurações dos ativos reparados ou substituídos estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos informando à COGEL/DITEC.
- **Teste de ambiente** - O ambiente principal do datacenter antes da recuperação dos dados do backup deverá ser testado a fim de garantir que o processo de recuperação ocorra conforme o planejado.
- Recuperar dados do backup - Proceder a recuperação dos dados para as aplicações, seja do storage ou de arquivos de backup.

12.3 Encerramento do PRD
Ao término do procedimento de recuperação, as informações de serviços serão consolidadas em parecer específico informando horário de reestabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

ANEXO VI

SALVADOR
PREFEITURA

Política de Segurança da Informação

Plano de Gerenciamento de Vulnerabilidades

PGV PMS - COGEL
V 1.0

Histórico de revisões

Versão	Data	Alteração
Versão 1.0	24/10/2023	Lançamento da Primeira versão adequada a PSI PMS

Sumário

1 Introdução 3
2 Objetivo 3
3 Aplicabilidade 3
4 Glossário de Termos e Definições Utilizados neste Documento 3
5 Referências Legais e de Boas Práticas 4
6 O Processo de Gerenciamento de Vulnerabilidades 4
6.1 Mapeamento de Ativos de Informação 5
6.2 Detecção de Vulnerabilidades 5
6.2.1 As principais ações relacionadas à detecção de vulnerabilidades têm os seguintes enfoques: 5
6.2.2 O processo de detecção de vulnerabilidade deve seguir as seguintes premissas: 6
6.2.3 Categorização das Vulnerabilidades 6
6.3 Elaboração e Manutenção de Relatórios 7
6.4 Banco de Dados de Vulnerabilidades 7
6.5 Tratamento das Vulnerabilidades 7
6.6 Das Exceções 9
6.7 Dos registros de Logs 9
6.8 Comunicação da ocorrência de vulnerabilidades e correções 9
6.9 Implementação e verificação das correções de vulnerabilidades 9
7 Dos serviços de nuvem ou de terceiros 10

1 Introdução
Gestão de vulnerabilidades é o processo de identificação, avaliação, priorização e mitigação de vulnerabilidades em sistemas, redes e computadores. O objetivo da gestão de vulnerabilidades é reduzir o risco de um ciberataque bem-sucedido e manter informações confidenciais seguras.
O Plano de Gerenciamento de Vulnerabilidade da PMS (PGV PMS) fornece os processos e procedimentos para governar o ciclo de vida da gestão de vulnerabilidades e assim garantir que os ativos da instituição não contenham vulnerabilidades. Esta política se aplica a todos os departamentos e todos os ativos conectados à rede institucional da Prefeitura Municipal de Salvador (PMS).

2 Objetivo
O objetivo do PGV é estabelecer as regras relacionadas às atividades de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades. Além disso, contempla ações e boas práticas que devem ser observadas para se evitar que vulnerabilidades estejam presentes nos ativos da organização.
A revisão, a avaliação, a aplicação e a verificação das atualizações de ativos de informação auxiliam a mitigar as vulnerabilidades no ambiente de Tecnologia da Informação e Telecomunicações, bem como os riscos associados a tais vulnerabilidades.

3 Aplicabilidade
O PGV PMS se aplica aos sistemas e ativos informacionais da PMS, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e/ou utilizem ativos informacionais. A presente política se aplica também a quaisquer provedores e entidades terceirizadas com acesso a informações, redes e aplicativos da PMS.
Os serviços de TI críticos da PMS devem ser formalmente elencados pela COGEL/DITEC. Esta é a responsável por elaborar, manter e fazer cumprir a Política de Gerenciamento de Vulnerabilidades no DATACENTER da PMS situado na COGEL.

4 Glossário de Termos e Definições Utilizados neste Documento
Ameaça – Conjunto de fatores externos com o potencial de causarem dano para um sistema ou organização;
Análise de Vulnerabilidades – Verificação e exame técnico de vulnerabilidades, para determinar onde estão localizadas e como foram exploradas;
Ativos de Informação – Meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;
Banco de Dados – Coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;
CVE (Common Vulnerabilities and Exposures) – Vulnerabilidades e Exposições Comuns;
CVSS (Common Vulnerability Scoring System) – Sistema comum de pontuação de vulnerabilidade;
HOST – Um computador ou dispositivo de TI (por exemplo, roteador, switch, gateway, firewall);
ID CVE – Identificação para um CVE específico;
Gerenciamento de Vulnerabilidades – Processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades;
Gestão de Mudanças na Segurança da Informação – Processo estruturado que visa aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;
LOG – Registro de eventos relevantes em um dispositivo ou sistema computacional. NTP (Network Time Protocol) – Protocolo de Tempo para Redes;
PATCH – Uma parte de código adicional desenvolvido para resolver um problema ou falha em um software existente;
Remediação – O ato de corrigir uma vulnerabilidade ou eliminar uma ameaça;

Risco – No sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;
Risco de Segurança da Informação – Risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
Teste de Invasão – Metodologia para testar a eficácia e a resiliência de ativos através da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante;
Teste de Penetração (PENTEST) – Também chamado de teste de intrusão, é fundamental para a análise de vulnerabilidades e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas ou pelas instituições detentoras dos softwares que estão sendo utilizados pelo órgão ou entidade;
Vulnerabilidade – Condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

5 Referências Legais e de Boas Práticas

No PGV PMS foram utilizadas as seguintes referências legais e de boas práticas:

- Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06;
- Framework de segurança cibernética do CIS 8 - Salvaguardas do controle 7 (Continuous Vulnerability Management), controle 11 (Data Recovery Capabilities), e controle 18 (Penetration Testing);
- Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI Gestão da Segurança da Informação;
- Controle 7 do Guia do Framework de Privacidade e Segurança da Informação, (p.45), https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf em 24/10/2023, "Gestão Contínua de Vulnerabilidades". Medidas 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7.;
- Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados - CAPÍTULO VII - Seção I – art. 46, Seção II - art. 50;
- Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI) em sua íntegra;
- Norma ABNT NBR ISO/IEC 27001:2022 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - A.12.3 Cópias de segurança;
- Norma ABNT NBR ISO/IEC 27002:2022 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação - 12.3 Cópias de segurança 18 Conformidade;
- National Institute of Standards and Technology (NIST) CSF: SP 800-40 Rev.2, Creating a Patch and Vulnerability Management Program CSF: SP 800-40 Rev 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology;
- Office of the Chief Technology Officer – OCTO - Política de gerenciamento de vulnerabilidades;
- Vulnerability Management Policy Template for CIS Control 7 em sua íntegra.

6 O Processo de Gerenciamento de Vulnerabilidades

Um processo de Gerenciamento de Vulnerabilidades (PGV PMS) deve ser criado, implementado, mantido e aplicado no DATACENTER da COGEL, obedecendo as seguintes premissas:

- O processo deve conter a implementação de mecanismos para obter informações oportunas sobre vulnerabilidades técnicas dos sistemas e ativos de informação, a avaliação da exposição da organização a tais vulnerabilidades e a implementação de salvaguardas apropriadas para lidar com o risco associado;
- O processo deve contemplar o gerenciamento de vulnerabilidades dos diversos ativos que sustentam os serviços da organização, como a ativos que compõe a rede da organização, aplicações web, aplicativos móveis, sistemas operacionais, dentre outros;
- O processo deve incluir atividades de suporte, incluindo, mas não se limitando a métricas de relatório e treinamento para implementação eficaz do PGV PMS;
- O processo deve incluir funções e responsabilidades das equipes/funções para realizar todas as atividades de maneira oportuna e eficaz para [o órgão ou entidade;
- O processo deve estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes;
- A consistência e a eficácia do processo devem ser medidas por meio de métricas de gerenciamento de vulnerabilidades.

As métricas de gerenciamento de vulnerabilidades devem ser definidas pelo Comitê Consultivo de Segurança da Informação (CCSI) e suas medições devem ser apresentadas a cada 6 meses. As métricas devem mensurar o grau de vulnerabilidade/ameaça em um determinado ativo de informação ou infraestrutura de TI, a exemplo de: cobertura, tempo de detecção, tempo de permanência, tempo para contenção ou atenuação, número médio de vulnerabilidades ao longo do tempo, eficiência no gerenciamento de patches e resultados de correção em relação aos SLAs da tabela de priorização de vulnerabilidades.
O Ciclo de Gestão de Vulnerabilidades deve conter as seguintes fases:

- Fase 1: Descoberta através do mapeamento de Ativos de Informação. Criação de um inventário completo com os ativos em toda a rede da instituição, para identificar quais ativos devem fazer parte do processo de gestão de vulnerabilidades. Identificar as vulnerabilidades existentes através de ferramenta automatizada a partir da varredura de sistemas que podem ser acessados por meio da rede corporativa. Identificar portas de entrada a esses sistemas, coleta e comparação das informações do sistema com vulnerabilidades conhecidas;
- Fase 2: Priorização De Ativos. Atribuir um grau de criticidade e importância aos ativos que compõem a infraestrutura de TI da empresa para definir quais devem ser prioridade no processo de análise e correção de vulnerabilidades;
- Fase 3: Avaliação. Avaliar os ativos para entender qual representa um risco maior à Segurança da Informação e, então, determinar quais riscos devem ser eliminados primeiro. Essa avaliação deve se basear em múltiplos critérios tais como a classificação baseada na pontuação CVSS, o nível de ameaça e a criticidade da vulnerabilidade;
- Fase 4: Correção. Efetuar as correções das vulnerabilidades identificadas e classificadas como críticas e urgentes. Uma vez que estas forem feitas, a equipe de segurança pode passar para as próximas, seguindo a lista de prioridades;
- Fase 5: Verificação E Monitoramento. Auditorias e de acompanhamento de todo o processo para assegurar sua eficácia na eliminação dos potenciais riscos.

6.1 Mapeamento de Ativos de Informação

Um mapeamento de ativos de informação deve constar no escopo do processo de gerenciamento de vulnerabilidades e patches para determinar qual marca, modelo e versão de equipamento de hardware, sistemas operacionais, banco de dados, sistema, servidor web e aplicativos de software.
O mapeamento de ativos de informação deve ser atualizado a cada 6 meses ou sempre que ocorrerem alterações significativas para garantir que os recursos informacionais estejam cobertos pelo processo de gerenciamento de vulnerabilidades do DATACENTER da COGEL.

6.2 Detecção de Vulnerabilidades

6.2.1 As principais ações relacionadas à detecção de vulnerabilidades têm os seguintes enfoques:

- definir e refinar o escopo que será avaliado;

- preparar as ferramentas necessárias e verificar sua integridade;
- realizar testes e verificar resultados;
- Reportar as vulnerabilidades identificadas em tempo hábil para sua correção.

6.2.2 O processo de detecção de vulnerabilidade deve seguir as seguintes premissas:

- As funções e as responsabilidades das equipes/funções para realizar atividades de detecção de vulnerabilidades devem ser estabelecidas;
- As ferramentas devem ser configuradas e ajustadas adequadamente de acordo com o escopo avaliado;
- Os tipos de varreduras e os tipos de teste devem ser avaliados e ajustados para que sejam congruentes com o escopo avaliado;
- A frequência de testes de segurança deve levar em consideração os requisitos legais, regulamentares e contratuais que a PMS deve cumprir e os riscos associados aos ativos avaliados;
- As varreduras de vulnerabilidades na rede corporativa devem ser realizadas por períodos determinados ou após alteração significativa na rede, por equipe interna ou por terceiro ou uma combinação de ambos;
- Os testes de segurança devem utilizar o feed de vulnerabilidade mais recente, de forma a evitar que determinadas vulnerabilidades não sejam detectadas;
- Para cada teste, é necessário verificar a integridade da ferramenta utilizada e se ela varreu corretamente os ativos analisados e se existem exceções de vulnerabilidades;
- As ferramentas utilizadas devem ser ajustadas continuamente, de forma a evitar que varreduras feitas por ferramentas distintas gerarem resultados distintos;
- O teste de invasão ou o teste de penetração (Pentest) deve ser realizado conforme critério de necessidade da PMS ou pelo menos a cada 6 meses, utilizando especialistas qualificados externos como parte de um exercício planejado, que inclui o escopo da avaliação, os métodos de uso e os requisitos operacionais, a fim de fornecer as informações mais precisas e relevantes sobre as vulnerabilidades atuais, sem afetar o funcionamento normal da PMS;
- A integridade do resultado de detecção de vulnerabilidades deve ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos;
- A detecção manual de vulnerabilidades deve ser considerada como complemento à detecção automática de vulnerabilidades.

6.2.3 Categorização das Vulnerabilidades

O PGV PMS considera o grau de risco de cada brecha de segurança. Essa avaliação é feita considerando a classificação baseada no Common Vulnerability Scoring System (CVSS); um sistema que define pontuações para indicar a gravidade e as características das vulnerabilidades de software. O sistema é um padrão gratuito e aberto que diversas empresas de segurança cibernética do mundo todo usam para avaliar e comunicar a gravidade e as características de alguma vulnerabilidade. E, para auxiliar no processo que favorece a tomada de decisões na gestão de vulnerabilidades, o NVD também disponibiliza uma biblioteca constantemente atualizada de vulnerabilidades e exposições comuns (CVEs), com classificações de gravidade e outras informações pertinentes como o nome do produto e sua versão.

A pontuação básica do CVSS varia de 0.0 a 10.0 e a categorização das vulnerabilidades também conta com uma classificação adicional incluída pelo National Vulnerability Database (NVD). As pontuações do CVSS v3.0 e as classificações associadas são as seguintes:

a) Pontuação CVSS 0.0 — gravidade: nenhuma;
b) Pontuação CVSS 0.1 a 3.9 — gravidade: baixa;
c) Pontuação CVSS 4.0 a 6.9 — gravidade: média;
d) Pontuação CVSS 7.0 a 8.9 — gravidade: alta;
e) Pontuação CVSS 9.0 a 10.0 — gravidade: crítica.

6.3 Elaboração e Manutenção de Relatórios

A Gerência Especial de Segurança (GES) deve elaborar relatórios após cada ciclo de detecção para auxiliar a COGEL/DITEC a entender e mensurar as vulnerabilidades existentes.

Os resultados da varredura devem passar por análise da GES com o dispositivo ou gerenciador de rede para que possíveis falsos positivos possam ser identificados e eliminados.

Grupos de ativos de informação devem ser determinados por tipo de ambiente, por tipo de sistema, por ID CVE ou por tipo de vulnerabilidade.

A GES deve adotar métricas para os relatórios de vulnerabilidade e determinar o valor percentual dos ativos de informação vulneráveis por gravidade e CVSS.

A quantidade e a porcentagem de novas vulnerabilidades devem ser monitoradas por: severidade; grupos funcionais; tipo de ambiente; tipo de sistema; autoridade de numeração CVE; e tipo de vulnerabilidade.

O relatório deve ser classificado, durante e após a sua elaboração, de acordo com a sensibilidade das informações presentes nele.

Todas as versões do relatório devem ser remetidas a COGEL/DITEC que o encaminhará ao Comitê Consultivo de Segurança (CCS).

6.4 Banco de Dados de Vulnerabilidades

É importante saber que o gerenciamento de vulnerabilidades deve ser capaz de produzir e manter um banco de dados de vulnerabilidades coletadas de todas as suas fontes.

Este banco de dados de vulnerabilidades poderá ser utilizado durante a priorização e a correção de vulnerabilidades.

Deve ser mantido um banco de dados de vulnerabilidades coletadas de várias fontes, como sites de segurança da informação, boletins de segurança ou publicações de fornecedores de software, que precisam ser aplicadas aos sistemas e ativos informacionais da COGEL/DITEC.

O banco de dados poderá incluir informações de vulnerabilidade, análise de vulnerabilidade para priorização e plano de correção de vulnerabilidade.

O banco de dados deve ser atualizado regularmente com as informações mais recentes. As novas vulnerabilidades devem ser adicionadas ao banco de dados tão logo forem descobertas.

É recomendável que o banco de dados de vulnerabilidades seja integrado com outras ferramentas de segurança, como scanners de vulnerabilidades e sistemas de gerenciamento de patches. Isso ajuda a identificar e corrigir vulnerabilidades de forma mais rápida e eficiente.

As informações coletadas no banco de dados de vulnerabilidades devem ser analisadas regularmente para identificar tendências e padrões visando a tomada de medidas proativas para evitar futuras vulnerabilidades. Priorização e correção de vulnerabilidades O monitoramento proativo de vulnerabilidades e ameaças em dispositivos, se remediadas, reduzirá ou eliminará o potencial de exploração e economizará os recursos necessários para responder a incidentes após a exploração.

6.5 Tratamento das Vulnerabilidades

O tratamento de vulnerabilidades deve ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo ou host impactado tem para o negócio da COGEL/DITEC.

As vulnerabilidades devem ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados abaixo:

Nível de Severidade	Prazo de Correção	Descrição do Risco
Muito Crítico (6)	Até 2 dias	Condição totalmente inaceitável quando medidas imediatas devem ser tomadas para eliminar a materialização do risco e mitigar perigos e impactos.
Crítico (5)	Até 30 dias	Pessoas mal-intencionadas podem facilmente obter o controle do host, o que pode comprometer toda a sua rede. As vulnerabilidades incluem acesso de leitura e gravação a arquivos, execução remota de comandos e backdoors.
Alto (4)	Até 45 dias	Pessoas mal-intencionadas podem obter o controle do host ou coletar informações altamente confidenciais, incluindo acesso de "leitura" ao arquivo, backdoors em potencial ou uma lista de todas as contas de usuário no host.
Médio (3)	Até 90 dias	Pessoas mal-intencionadas podem obter acesso às configurações de segurança no host, o que pode levar ao acesso a arquivos e à divulgação de conteúdo de arquivos, navegação em diretórios, ataques de negação de serviço e uso não autorizado de serviços.
Baixo (2)	Até 120 dias	Pessoas mal-intencionadas podem coletar informações confidenciais do host, como versões de software instaladas, que podem revelar vulnerabilidades conhecidas.
Muito baixo (1)	Até 180 dias	Pessoas mal-intencionadas podem coletar informações sobre o host por meio de portas ou serviços abertos, o que pode levar à divulgação de outras vulnerabilidades. É fundamental que o órgão ou a entidade seja capaz de estabelecer essa classificação de risco de acordo com suas demandas e necessidades internas.

Os testes que forem concluídos com falha devem ser examinados novamente até que sua execução seja concluída com êxito. Caso não seja possível, deve-se avaliar se a vulnerabilidade será incluída na lista de exceções por pessoal autorizado, com base no processo de aceitação de risco.
Devem-se estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente, utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.
Quando as vulnerabilidades não puderem ser corrigidas dentro do prazo estabelecido, a GES deve enviar uma ocorrência a COGEL/DITEC. A ocorrência deve conter as seguintes informações:

- Detalhes do sistema ou ativo;
- Descrição detalhada da vulnerabilidade;
- Avaliação de risco que justifique a não correção imediata;
- A justificativa clara pela qual a correção não pode ser realizada no prazo estabelecido;
- Detalhes dos controles existentes (se houver);
- Novo prazo de correção;
- Plano de ação da remediação (obedecendo o novo prazo de correção).

A decisão de aceitar ou rejeitar a ocorrência deve ser tomada pela COGEL/DITEC com base na avaliação de risco apresentada. Se a ocorrência for aceita, a vulnerabilidade deve ser monitorada continuamente, pautado pelo plano de ação apresentado devendo ser corrigida assim que possível.
Os alertas de vulnerabilidades, as correções de patches e as ameaças emergentes que correspondam aos recursos informacionais relacionados ao inventário de sistema e ativos de informação devem ser monitorados.

6.6 Das Exceções
As exceções à política de gerenciamento de vulnerabilidades devem ser tratadas de forma transparente e consistente, minimizando os riscos potenciais e protegendo adequadamente os ativos de informação da organização.
Para os ativos de informação não contemplados por esta política em função de dificuldades técnicas ou obrigações contratuais e normativas ou outras razões legítimas, as exceções deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções da COGEL/DITEC.
A lista de exceções de ativos de informação deve ter validade de 6 meses, devendo ser revisada após esse período.

6.7 Dos registros de Logs
Identificar quais eventos dos ativos de informação devem ser registrados, com base nos requisitos regulatórios, nas melhores práticas e nos objetivos da COGEL/DITEC.
Ativos, físicos ou virtuais, como servidores e recursos de rede, devem recuperar informações baseadas em tempo de uma única fonte de tempo de referência (servidor NTP) regularmente para que os relógios de registro sejam consistentes.
As configurações referentes a ativos de informação devem incluir configurações de log para registrar ações que possam afetar ou que sejam relevantes para a segurança da informação.
Definir procedimento para análise de logs, como ferramentas de análise e correlação, para identificar possíveis ameaças e vulnerabilidades.
Uma revisão dos arquivos de registro (logs) deve ser conduzida pelo menos por um ano.
Os arquivos de registro (logs) devem ser protegidos contra adulteração e acesso não autorizado ou exfiltração.
Registros de logs dos sistemas e ativos informacionais classificados como críticos devem ser mantidos por pelo menos por 2 anos, tempo suficiente para cumprir os requisitos regulatórios e permitir a detecção de ameaças passadas.
Monitorar regularmente os registros de logs para identificar quaisquer tentativas de exploração de vulnerabilidades.
Registros de log devem ser excluídos de forma segura, garantindo que os registros sejam completamente apagados sem deixar vestígios ou dados remanescentes.

6.8 Comunicação da ocorrência de vulnerabilidades e correções
As vulnerabilidades e respectivas informações de correção devem ser informadas aos usuários afetados, incluindo, mas não se limitando a: administradores de sistema, proprietários de sistema e usuários finais.
As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio de verificação de vulnerabilidades de rede e host, verificação de logs de patches, testes de invasão/penetração (Pentest) e verificação das definições de configuração.

6.9 Implementação e verificação das correções de vulnerabilidades
A implementação e verificação das correções de vulnerabilidades envolvem um processo contínuo e iterativo de identificação, correção e monitoramento das vulnerabilidades para garantir a proteção contra ameaças de segurança da informação.
As correções de vulnerabilidades devem ser verificadas a saber se não há novas vulnerabilidades introduzidas. Isso pode ser feito por meio de testes de penetração, testes de vulnerabilidade e análise de logs.
Somente correções de vulnerabilidades que foram efetivamente testadas e aprovadas devem ser implantadas em produção. Atividades de correção de vulnerabilidades geralmente incluem, mas não se limitam à instalação de patches de segurança, bem como a ajustes de configuração e/ou remoção de software.
Quando instalações de patches de segurança e ajustes de configuração são recomendadas para mitigar as vulnerabilidades, elas devem ser enviadas a GES para que os controles apropriados sejam implementados para teste, avaliação de riscos e reparação.

7 Dos serviços de nuvem ou de terceiros
Para serviços em nuvem, as responsabilidades do provedor de serviços em nuvem pública com o cliente do serviço em nuvem devem ser definidas e acordadas. Terceiros devem cumprir os requisitos desta Política de Gerenciamento de Vulnerabilidades (PGV PMS).
Sempre que possível, essa obrigação e outras responsabilidades que envolvam o gerenciamento de vulnerabilidades devem ser incluídas em contratos com terceiros.

ANEXO VII

Política de Segurança da Informação

Plano de Resposta a Incidentes de Segurança

PRI PMS - COGEL
V 1.0

Histórico de revisões

Versão	**Data**	**Alteração**
Versão 1.0	10/11/2023	Lançamento da Primeira versão adequada a PSI PMS

Sumário

1 Introdução 3
2 Objetivo 3
3 Aplicabilidade 3
4 Glossário de Termos e Definições Utilizados neste Documento 3
5 Referências Legais e de Boas Práticas 4
6 Tratamento de Incidentes Cibernéticos 5
6.1 Triagem 5
6.2 Análise 6
7 Resposta a Incidentes 6
7.1 Contenção 6
7.2 Erradicação 7
7.3 Recuperação 7
8 Incidentes envolvendo Dados Pessoais 7
9 Pós-Incidente 8
9.1 Melhoria Contínua dos Processos 8

1 Introdução

Os incidentes cibernéticos precisam ser continuamente enfrentados para garantir que a disponibilidade, a integridade, a confidencialidade e a autenticidade dos serviços e das informações sejam preservadas. Especialmente, um incidente cibernético em ativo de informação governamental pode causar grave impacto negativo para a sociedade.

2 Objetivo

O objetivo do PRI PMS é Orientar a Prefeitura Municipal de Salvador (PMS) nas respostas aos incidentes de segurança da informação, de forma documentada, formalizada, rápida e confiável, resguardando as evidências que possam ajudar a prevenir novos incidentes e a atender às exigências legais de comunicação e transparência.

Além disso, busca-se atingir os seguintes objetivos específicos:

- Conferir clareza sobre o fluxo de procedimentos adequados e os responsáveis, no caso de incidentes;
- Assegurar respostas rápidas, efetivas e coordenadas;
- Evoluir continuamente com as lições aprendidas.

Este plano estabelece etapas acionáveis, com linhas de comunicação, funções e notificações necessárias para responder a qualquer violação de segurança.

3 Aplicabilidade

O PRI PMS se aplica aos sistemas e ativos informacionais da PMS, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e/ou utilizem ativos informacionais. A presente política se aplica também a quaisquer provedores e entidades terceirizadas com acesso a informações, redes e aplicativos da PMS.

O registro e controle dos incidentes de segurança da informação da PMS devem ser formalmente comunicados à COGEL/DITEC por qualquer notificador. Esta é a responsável por elaborar, manter e fazer cumprir o Plano de Resposta a Incidentes de Segurança da PMS

4 Glossário de Termos e Definições Utilizados neste Documento

Acionador - Grupo ou responsável que receberá notificações de incidentes em primeira mão para triagem, estruturado em níveis distintos para viabilizar a importante cobertura 24 horas;

Ataque - Evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

Ativo comprometido ou Alvo: Dispositivo, sistema, ou recurso que seja acessado, modificado ou utilizado de forma não autorizada por indivíduos maliciosos ou não autorizados;

Autoridade Nacional de Proteção de Dados (ANPD) - É o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro;

Controlador - É toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais;

Dados Pessoais - Qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, por conta própria ou quando combinada com outras informações;

Dados Pessoais Sensíveis - São dados pessoais que digam respeito a 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, quando vinculado a uma pessoa natural;

Desenvolvedores/Operadores/Fornecedores dos sistemas - Atuam no desenvolvimento de solução e instalação dos sistemas;

Encarregado pelo Tratamento de Dados Pessoais (DPO) - Responsável por encaminhar comunicações formais em incidentes envolvendo vazamentos de dados pessoais. Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Incidente - Qualquer evento que não faça parte da operação padrão de um serviço/atividade e que cause ou possa causar uma interrupção ou redução, não planejada, da qualidade do serviço/atividade;
Incidente de segurança - Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
Incidente de segurança com dados pessoais - De acordo com a ANPD, incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares de dados pessoais;
Notificador - Pessoa ou sistema de monitoração que notifica incidente;
Responsável por Sistema ou Controlador de Sistema - Indicado que deve ser contatado e com poder para autorizar ou vetar procedimentos de emergência.

5 Referências Legais e de Boas Práticas

No PRI PMS foram utilizadas as seguintes referências legais e de boas práticas:

- Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal – PLANGIC plangic.pdf (www.gov.br) - Portaria DSI/GSI/PR Nº 120 de 21 de Dezembro de 2022, acesso em 24/10/2023.
- Plano de Resposta a Incidentes de Segurança – TRT 15 - https://trt15.jus.br/sites/portal/files/roles/institucional/gestaoestrategica/lgpd/Plano%20de%20Resposta%20a%20Incidentes%20de%20Seguran%C3%A7a.pdf, acesso em 24/10/2023.

6 Comunicação de Incidentes

Um novo incidente é notificado por qualquer usuário da PMS (notificador) ou por alarme da monitoração. A comunicação inicial do incidente pode ser proveniente de qualquer fonte por intermédio do GLPI, por manifestações escritas através de e-mail (que serão inseridas no sistema eletrônico), pessoalmente, ou, ainda, por telefone. A identificação de um incidente também pode ocorrer pela interrupção não planejada de um serviço de TI; por recebimento de e-mails com links suspeitos para clicar ou contendo código malicioso, o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda; entre outras ocorrências suspeitas como vírus, ataques cibernéticos e outros.
Nesta etapa, sugere-se que o incidente seja documentado em base de conhecimento apropriada, detalhando as informações obtidas, linha do tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.
Ao se registrar uma notificação de incidente de segurança da informação, deve-se inserir as seguintes informações para controle e armazenamento:

a) Origem do incidente: unidade, setor ou organização à qual o dispositivo ou o processo que originou o incidente pertence;
b) Contato da origem: e-mail, telefone ou outro contato disponível do informante do incidente;
c) Registro do tempo da ocorrência do incidente: data e hora em formato GMT (Greenwich Mean Time) na qual o incidente foi identificado. Exemplo: "10:23, 20 de março de 2023";
d) Local onde originou o incidente: endereço IP (IPv4 ou IPv6) do dispositivo ou serviço que originou o incidente;
e) Recursos utilizados pela origem do incidente: especificação do tipo do protocolo (IP, TCP, UDP etc.) e portas, ou procedimentos operacionais, adotados na ação do incidente;
f) Endereço do ativo comprometido: endereço IP (IPv4 ou IPv6) do dispositivo ou endereço de acesso do serviço que foi o alvo do incidente;
g) Protocolos e portas alvos do incidente: especificação do tipo do protocolo (IP, TCP, UDP etc.) e portas utilizados no destino do incidente;
h) Serviços envolvidos: especificação do serviço que foi alvo do incidente (HTTP, FTP, SMTP etc.) e versões de sistemas utilizados;
i) Aplicações afetadas: descritivo de quais serviços da Prefeitura Municipal de Salvador possuem relações e/ou foram afetados pelo incidente, se houve indisponibilidade completa ou parcial do serviço;
j) Descrição do incidente: breve descrição do incidente, tais como tipo do ataque, motivação aparente, ou outras características relevantes;
k) Logs ou evidências: anexação das porções de log, imagens, códigos de erro ou outros registros que evidenciem a ocorrência do incidente.

7 Tratamento de Incidentes

O Processo de Tratamento de Incidentes inicia-se imediatamente após a detecção ou a notificação de provável ocorrência destes, pelo processo de triagem, seguido pelo processo de análise.

7.1 Triagem

A etapa de triagem tem como objetivo reunir informações sobre o evento, avaliar a sua natureza, e classificá-lo como incidente para que, adiante, se inicie o processo de tratamento. O processo de triagem consiste em:

- Classificar o tipo de incidente;
- Verificar se há correlação com outros incidentes;
- Estabelecer uma criticidade e prioridade para o tratamento do incidente;
- Registrar e definir o andamento do incidente na base de incidentes;
- Atribuir o tratamento do incidente ao analista ou à equipe responsável;
- Comunicar formalmente aos setores envolvidos;

A **Classificação** do incidente é importante para esclarecer e auxiliar no tipo de atendimento a ser realizado e na definição da sua criticidade. As classificações sugeridas neste Plano são:

1. **Conteúdo abusivo**: spam, assédio etc.;
2. **Código malicioso**: bot, worm, vírus, trojan, spyware, scripts;
3. **Prospecção por informações**: varredura, sniffing, engenharia social;
4. **Tentativa de intrusão**: tentativa mal-sucedida de exploração;
5. **Intrusão**: Acesso lógico indesejável, comprometimento de conta de usuário, de aplicação;
6. **Indisponibilidade de serviço ou informação**: negação de serviço, sabotagem;
7. **Comprometimento da informação**: acesso não-autorizado à informação, modificação não autorizada da informação;
8. **Fraude**: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada;
9. **Outros**: incidente não categorizado.

O estabelecimento da **Criticidade** tem como objetivo definir uma ordem de atendimento dos incidentes e um SLA (Service Level Agreement - Acordo de Nível de Serviço) de acordo com a urgência de tratamento e o impacto nas áreas administrativas da PMS. Assim, sugere-se determinar a classificação de criticidade do incidente de acordo com as definições a seguir:

1. **Crítico -** Incidente paralisa os serviços da PMS comprometendo as áreas operacionais da organização;
2. **Alto -** Incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a PMS;
3. **Médio -** Incidente que afeta sistemas ou informações não críticas, sem impacto negativo a PMS;
4. **Baixo –** Suspeita de possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

O estabelecimento de prioridades se dará em função da criticidade do incidente, a estratégia de negócio da unidade, área de atuação, cadeia de suprimentos, geolocalização e outros fatores considerados relevantes. Após estabelecer essa priorização, o incidente será classificado de acordo com o impacto na disponibilidade, integridade, confidencialidade e autenticidade.
A definição da **Situação** do incidente tem como objetivo permitir o acompanhamento do andamento de tal evento dentro do processo de tratamento. De acordo com este plano, os incidentes podem ter os seguintes status situacionais:

1. **Aberto**: nesse momento foi realizado apenas o registro das informações;
2. **Processamento**: o chamado é assumido por um técnico e está em tratamento;

3. **Pendente**: necessário confirmar alguma informação com o solicitante antes de dar prosseguimento. Tentativas de contato devem ser realizadas e registradas;
4. **Transferido** (pendente de terceiros): ocorre quando uma equipe solucionadora não tem ação no chamado, o qual é repassado;
5. **Solucionado**: indica que o procedimento técnico foi aplicado e aparentemente o chamado foi solucionado;
6. **Fechado**: a solução do chamado foi confirmada pelo solicitante. O fechamento pode ocorrer automaticamente ou por contato.

7.2 Análise

O processo de análise consiste nas seguintes atividades listadas abaixo:

- Validação: validar as informações tratadas na triagem, ratificando-as, complementando-as ou retificando-as;
- Causa raiz: identificar e avaliar atividades anômalas em relação à linha de base conhecida;
- Ataque: identificar pelo menos uma parte da cadeia de ataque para permitir a definição das atividades de resposta;
- Colaboração: complementar e adicionar novos dados a partir da colaboração das fontes utilizadas na detecção; e
- Documentação: incluir todos os dados coletados na documentação sobre o incidente para viabilizar as ações de pós-incidente.

8 Resposta a Incidentes

O processo de resposta a um incidente consiste em ações de:

- contenção;
- erradicação; e
- recuperação.

As ações de contenção, erradicação e recuperação devem ser baseadas nos seguintes critérios:

- criticidade dos ativos afetados;
- tipo e gravidade do incidente;
- necessidade de preservar a evidência;
- importância de quaisquer sistemas afetados para processos de negócio críticos; e
- recursos necessários para implementar a estratégia.

A Gerência Especial de Segurança (COGEL/DITEC/GES) deverá encaminhar, tempestivamente, em função do tipo e do impacto, os dados relativos ao incidente cibernético para a diretoria da COGEL/DITEC, os quais deverão ser analisados em conjunto com a área jurídica do órgão ou da entidade, de forma que sejam adotadas as medidas legais, administrativas e cíveis cabíveis, incluindo a comunicação com as autoridades policiais competentes.
Havendo exfiltração de dados pessoais, o encarregado de dados pessoais da COGEL deverá informar à Autoridade Nacional de Proteção de Dados (ANPD), de acordo com os procedimentos previstos em legislação, normativos e orientações.

8.1 Contenção

O objetivo da contenção é limitar os danos causados pelo atual incidente de segurança e evitar outros. Devem ser aplicadas medidas para mitigar o incidente, evitando-se a destruição de provas que possam servir de subsídios para possível processo cível, penal ou administrativo. A ação de contenção poderá envolver as seguintes atividades:

- contenção a curto prazo, que consiste em:
  - Limitar os danos antes que o incidente piore;
  - Isolar segmentos de rede; e
  - Executar um failover routing (desvio de tráfego de rede para os recursos que estejam saudáveis e disponíveis);
- realização de imagem forense do ambiente afetado; e
- contenção a longo prazo, que consiste em:
  - Identificar vulnerabilidades exploradas pelos atacantes e os mecanismos que permitiram o ataque; e
  - Aplicar correções temporárias que permitam a volta ao funcionamento dos sistemas afetados.

8.2 Erradicação

A erradicação consiste em remover ou inutilizar artefatos utilizados pelos atacantes e em restaurar o ambiente afetado.
A ação de erradicação poderá envolver as seguintes atividades:

- restauração completa das imagens de unidades de armazenamento, implicando na exclusão de todos os dados atuais;
- recuperação dos dados a partir dos backups existentes;
- identificação das causas principais que originaram o ataque;
- realização dos procedimentos necessários para limpar a unidade de armazenamento, removendo ou isolando os artefatos utilizados pelos atacantes; e
- correção das vulnerabilidades encontradas.

8.3 Recuperação

O objetivo da recuperação é restabelecer o pleno funcionamento do ambiente afetado após garantir que as ameaças foram neutralizadas ou removidas. A ação de recuperação poderá envolver as seguintes atividades:

- definição de cronograma para a restauração das operações pelos responsáveis pelos ativos de informação afetados;
- realização de varredura completa do ambiente recuperado, de forma a garantir que este esteja apto para uso seguro;
- realização de testes de funcionamento do ambiente recuperado, validando os resultados com as linhas de base definidas, à medida em que estarão novamente disponibilizados para uso; e
- monitoramento do ambiente recuperado, a ser executado num período após o incidente cibernético, de forma a verificar comportamentos atípicos ou anormalidade nas operações.

Após o término do processo de recuperação, deverá ser elaborado um relatório do incidente, contendo as seguintes informações:

- atores atacantes e atacados;
- atores envolvidos no tratamento e resposta do incidente;
- evidências coletadas;
- indicadores de comprometimento (IoCs), bem como táticas, técnicas e procedimentos (TTPs);
- ativos de infraestrutura, serviços e total de usuários afetados;
- volume de dados exfiltrados;
- cronologia dos fatos;
- medidas de contenção, erradicação e recuperação adotadas; e
- medidas preventivas propostas para ocorrências similares.

9 Incidentes Envolvendo Dados Pessoais

Conforme o art. 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e 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, e tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução.
O art. 48 da LGPD determina que o Controlador tem a obrigação de comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que venha a gerar risco ou dano considerado relevante aos titulares. Todavia, a ANPD afirma que, embora a responsabilidade e a obrigação pela comunicação do incidente sejam do Controlador, podem ocorrer casos excepcionais em que tal comunicação provenha do Operador, caso em que tal comunicação será devidamente analisada pela ANPD.
A Autoridade Nacional de Proteção de Dados recomenda ainda (enquanto pendente a regulamentação), conforme Decreto nº 9936/2019, que o **prazo razoável para a comunicação de incidente** seja de **dois dias úteis.** Reforça que os Controladores tenham cautela quanto ao julgamento acerca da relevância dos riscos e danos referentes ao incidente e, em caso de dúvida, realizem a comunicação do incidente o mais breve possível para que não ocorra eventual descumprimento da LGPD.
A comunicação à ANPD deve conter no mínimo:

- a descrição da natureza dos dados pessoais afetados;
- as informações sobre os titulares envolvidos;
- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- os riscos relacionados ao incidente;
- os motivos da morosidade, no caso de a comunicação não ter sido imediata; e
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do dano causado.

10 Pós-Incidente

O objetivo desta fase é realizar a análise da documentação dos incidentes, do processo de comunicação e das regras de proteção do ambiente para evitar incidentes semelhantes e aperfeiçoar os processos existentes.
Os principais objetivos da análise pós-incidente incluem:

- confirmar que a causa raiz foi eliminada ou mitigada;
- estabelecer medidas preventivas para incidentes similares;
- identificar os erros ou ausências de infraestrutura a serem resolvidos;
- identificar as oportunidades de melhoria na política organizacional, normativos ou nos processos;
- revisar e atualizar as funções, as responsabilidades, o processo de comunicação e a autoridade da ETIR para garantir a resposta oportuna e adequada;
- identificar necessidades de treinamento técnico ou operacional;
- melhorar as ferramentas, ações e capacidades necessárias para realizar a prevenção, a detecção, o tratamento e a resposta;
- adicionar outros critérios para detecção e triagem da ameaça; e
- identificar e propor soluções para situações omissas verificadas no incidente.

10.1 Melhoria Contínua dos Processos

No intuito de evoluir em maturidade e nas ações perante incidentes cibernéticos, a GES deverá realizar a análise dos processos de prevenção, detecção, tratamento e resposta do incidente, de acordo com o Ciclo de melhoria na gestão de incidentes cibernéticos
A Figura 1 representa o ciclo de melhoria contínua, representado no anel interno, que ocorre simultaneamente com os processos de gestão de incidentes cibernéticos, representado no anel externo.

Figura 1 - Ciclo de Melhoria Contínua

DECRETOS SIMPLES

RETIFICAÇÃO

No Decreto s/nº de15/01/2024, publicado no DOM de 16/01/2024, referente a nomeação de **MÁRCIO LADEIA FERNANDES**,

Onde se lê:

... Gerente IV, Grau 57, da Diretoria Administrativa, ...

Leia-se:

... Gerente IV, Grau 57, da Gerência de Aquisições e Logística, da Diretoria Administrativa, ...

RETIFICAÇÃO

No Decreto s/nº de 08/01/2024, publicado no DOM de 09/01/2024, referente a exoneração de **JANDIRA FELIX DOREA**,

Onde se lê:

Exonerar, a pedido, **JANDIRA FELIX DOREA**, ...

Leia-se:

Exonerar, a pedido, **JANDIARA FELIX DOREA**, ...