INSTRUÇÃO NORMATIVA CGGDIESP-5/PGDI, de 27-12-2022

APROVA Instrução Normativa CGGDIESP-5/PGDI referente ao Anexo II, 3 – Tabela de Providências Complementares e Responsáveis – Armazenamento seguro de dados e informações: **Orientação Técnica - Procedimentos para segurança física de armazenamento de dados e informações**, da Deliberação Normativa CGGDIESP-1, de 30/12/2021.

ORIENTAÇÃO TÉCNICA

Procedimentos para segurança física de armazenamento de dados e informações

1. Objetivos

Esta orientação técnica tem os seguintes objetivos:

- Uniformizar normas e procedimentos para a segurança física de armazenamento de dados e informações, em atendimento à vigésima quarta providência requerida pela Política de Governança de Dados e Informações (PGDI) no âmbito da Administração Pública estadual, instituída pela Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021.
- Disseminar a importância da adoção de controles para a preservação do ambiente físico que protege os equipamentos, os sistemas de informação e as pessoas, bem como de controle de acesso a esses ambientes, em atendimento à vigésima quarta providência requerida pela Política de Governança de Dados e Informações (PGDI) no âmbito da Administração Pública estadual, instituída pela Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021.

2. Sumário

1. Objetivos
2. Sumário
3. Abrangência
4. Principais documentos relacionados e referenciais bibliográficos
5. Glossário
6. Contexto
7. Relação de temas abordados
8. Descrição das orientações técnicas (diretrizes, regras e/ou procedimentos)
8.1. Proteção perimetral
8.2. Controles de acesso físico
8.3. Controles de áreas de acesso comum
8.4. Controles de áreas seguras ou de acesso restrito
8.4.1. Identificação de área de acesso restrito
8.5. Controles de docas, depósitos e almoxarifados

8.5.1. Identificação de doca, depósito ou almoxarifado

8.5.2. Recepção em doca, depósito ou almoxarifado

8.5.3. Despacho em doca, depósito ou almoxarifado

8.5.4. Controle de correio ou malote

8.5.5. Controle de almoxarifado e depósito

8.6. Proteção contra ameaças externas e monitoramento de intrusão

8.7. Outras medidas requeridas pela PGDI

3. Abrangência

Órgãos e entidades da Administração Pública estadual.

4. Principais documentos relacionados e referenciais bibliográficos

- Política de Governança de Dados e Informações (PGDI), considerando, em seu Anexo II, as providências relacionadas aos controles para identificação e registro de acessos a ambientes físicos (vigésima terceira providência) e aos procedimentos para segurança física de armazenamento de dados e informações (vigésima quarta providência).
- Orientação Técnica do COETIC que instrui sobre "inventário de *hardware* e de *software*", conforme décima terceira providência requerida pela PGDI, em seu Anexo II.
- Orientação Técnica do CGGDIESP sobre melhores práticas de "gestão de riscos de segurança da informação", conforme trigésima providência requerida pela PGDI, em seu Anexo II.
- Lei Federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).
- Decreto Estadual nº 64.790, de 13 de fevereiro de 2020, que institui a Central de Dados do Estado de São Paulo – CDESP, a Plataforma Única de Acesso – PUA e o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo – CGGDIESP, e dá providências correlatas.
- Decreto Estadual nº 65.347, de 9 de dezembro de 2020, que dispõe sobre a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), no âmbito do Estado de São Paulo.
- DAMA INTERNATIONAL. *Data management body of knowledge – DAMA-DMBOK2.* 2. ed. Basking Ridge (NJ, EUA): Technics Publications, 2017.
- Normas Técnica ABNT NBR ISO/IEC Família 27000.

5. Glossário

Termos e siglas	Definição
CDESP	Central de Dados do Estado de São Paulo. Instituída pelo Decreto nº 64.790/2020, constitui repositório eletrônico de dados e informações, estruturados ou não, gerados ou coletados pela Administração Pública Estadual.
CFTV	Circuito Fechado de Televisão. Refere-se à infraestrutura de câmeras de vigilância do local.

Termos e siglas	Definição
CGGDIESP	Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo. Órgão colegiado de caráter consultivo, normativo e deliberativo, responsável pela gestão da CDESP e por auxiliar o controlador no desempenho das atividades indicadas no artigo 3º do Decreto Estadual nº 65.347/2020.
CPD	Centro de Processamento de Dados.
LGPD	Lei Geral de Proteção de Dados – Lei nº 13.709/2018. Promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo, essa Lei rege o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.
PGDI	Política de Governança de Dados e Informações. Instituída pela Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021, publicada no DOE de 31 de dezembro de 2021, que estabelece parâmetros para as boas práticas em segurança da informação, para a privacidade e proteção de dados pessoais e para a gestão de dados e informações, de observância obrigatória pelos Órgãos e Entidades da Administração Pública estadual.
PPDP	Política de Proteção de Dados Pessoais. Instituída pela Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021, publicada no DOE de 31 de dezembro de 2021, e corresponde à compilação de normas e regras de boas práticas de governança e proteção para tratamento de Dados Pessoais, de observância obrigatória pelos Órgãos e Entidades da Administração Pública estadual.
RFID	*Radio Frequency Identification* (Identificação por Radiofrequência). Trata-se de tecnologia usada, por exemplo, em *chips* de cartões de crédito e *chips* colocados em malotes e/ou embalagens cujo conteúdo está registrado.
SSCTI	Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação da Secretaria de Governo do Estado de São Paulo.
TIC	Tecnologia da Informação e Comunicação.
Token	Algo que o usuário possui e controla (tipicamente uma chave, senha e/ou módulo criptográfico) que é utilizado para autenticar a identidade do requerente e/ou a requisição em si.

6. Contexto

As ações para adequação aos preceitos da LGPD e às boas práticas de governança de dados e informações dispostas na PGDI e na PPDP e em seus respectivos Anexos II e III implicam a implementação, de forma ampla e transversal, de políticas, diretrizes, normas, metodologias, processos, procedimentos e tecnologias de TIC direcionadas à governança, à segurança e à proteção das informações e dos dados, inclusive dos dados pessoais e dos dados pessoais sensíveis, resultando em ações inter-relacionadas e indissociáveis.

A Gestão da Segurança da Informação é um processo voltado para o gerenciamento dos mecanismos de proteção e controle dos sistemas de informação, por meio de um conjunto de políticas e procedimentos direcionados aos ambientes digital e físico, para gerir sistematicamente riscos e exposições de dados e informações, visando à preservação da confidencialidade, da integridade, da autenticidade e da disponibilidade das informações, bem como à auditabilidade dos sistemas de tratamento de dados.

Promover de forma ampla a segurança da informação ultrapassa o fator computacional, e assegurar a proteção do ambiente físico segue a mesma abordagem utilizada para as informações digitais: definir o contexto, avaliar os riscos e implementar os mecanismos de proteção e controle mais

apropriados. O controle de acesso físico, por exemplo, é fundamental para monitorar a entrada e a saída de pessoas, ação que impacta diretamente a exposição das informações e da infraestrutura. As medidas de segurança física e controle de acesso físico visam impedir, detectar, defender, bloquear e corrigir invasões da instalação e de áreas críticas onde se encontrem ativos da informação sensíveis para a instituição, bem como proteger os ativos informacionais contra riscos naturais relacionados a incêndios, inundações e desmoronamentos, entre outros.

Para evitar eventuais problemas e diminuir ou eliminar as vulnerabilidades relacionadas aos diversos riscos inerentes aos ativos físicos e lógicos, independentemente da quantidade e relevância dos dados a serem protegidos, são recomendadas nesta orientação técnica soluções de infraestrutura, observando-se, contudo, que tal conjunto não se estabelece como modelo único, visto que cada órgão ou entidade tem características físicas particulares. Ressalta-se que, quanto maior for o nível de segurança necessário, mais barreiras físicas serão necessárias.

7. Relação de temas abordados

- Proteção perimetral.
- Controles de acesso físico.
- Controles de áreas de acesso comum.
- Controles de áreas seguras ou de acesso restrito.
- Controles de docas, depósitos e almoxarifados.
- Proteção contra ameaças externas e monitoramento de intrusão.

8. Descrição das orientações técnicas (diretrizes, regras e/ou procedimentos)

Conforme a Norma Técnica ABNT-NBR ISO/IEC 27002:2022 – Segurança da Informação, Segurança Cibernética e Proteção à Privacidade — Controles de Segurança da Informação, no seu capítulo 7, os controles e procedimentos de segurança física devem ser definidos e usados para proteger áreas que contenham informações e ativos de TIC, com o propósito de evitar: a) o acesso físico não autorizado; b) danos; e c) interferências nas informações, nos dados e em ativos associados. A norma também orienta, no seu capítulo 7.4, que as instalações sejam monitoradas continuadamente para detectar e impedir o acesso físico não autorizado. Da mesma forma, no seu capítulo 7.6, orienta que convém que a proteção contra ameaças físicas e ambientais, como desastres naturais, e outras ameaças físicas intencionais ou não intencionais à infraestrutura, seja projetada e implementada.

A seguir estão relacionadas orientações para a implementação de controles para identificação e registro de acessos aos ambientes físicos do órgão ou entidade e para a segurança física de armazenamento de dados e informações.

8.1. Proteção perimetral

A proteção perimetral é um método de segurança patrimonial com o objetivo de criar barreiras em torno de determinado lugar. Para tanto, é importante que existam infraestrutura física e edificações voltadas a impedir acessos físicos não autorizados e danos e interferências nos recursos tecnológicos e nas informações da instituição. A seguir, estão elencadas as principais barreiras e equipamentos relacionados aos temas de infraestrutura física e edificações necessários para impedir que pessoas não autorizadas acessem um local indevidamente.

- Barreiras físicas:
    - muros e alambrados;
    - cercas de proteção e/ou elétricas;
    - portas e portões;
    - especificações técnicas de construção civil e alvenaria para incremento do isolamento de áreas de acesso controlado, como espessura das paredes, *slab-to-slab*, blindagem de portas e janelas, grades de proteção em janelas (nos andares mais baixos) etc.;
    - guaritas e torres de vigilância.
- Acesso de veículos:
    - vias de acesso;
    - portão;
    - cancela;
    - estacionamento etc.
- Portas de entrada e saída e janelas:
    - trancas e fechaduras em portas, portões e janelas;
    - catracas e torniquetes;
    - clausuras e eclusas;
    - barras antipânico nas saídas de emergência etc.
- Iluminação externa:
    - postes;
    - luzes de emergência etc.
- Sinalização:
    - indicadores de percurso;
    - áreas de restrição;
    - alertas de segurança;
    - rotas de saídas de emergência etc.

- Pessoal de vigilância e emergência treinado.

8.2. Controles de acesso físico

Controle de acesso físico é qualquer sistema, mecanismo, equipamento ou procedimento que limite o acesso de alguém a determinado ambiente e às tecnologias de tratamento de dados. O objetivo é garantir a segurança de dados sigilosos, bens e pessoas. Os controles de acesso físico devem gerenciar o acesso de pessoas, veículos e materiais a locais e edificações, ou seja, controlar o fluxo de pessoas com a ajuda de dispositivos como:

- controladores de acesso físico:
    - fechaduras, trancas, cadeados;
    - chaves etc.;
- controladores de acesso eletrônico:
    - leitores de crachás;
    - teclados alfanuméricos;
    - leitores biométricos;
    - detectores de metal;
    - escâneres de raios X etc.;
- processos e rotinas para controle de chaves e cadeados físicos:
    - custódia e guarda de chaves físicas de cadeados e fechaduras;
    - acesso e troca de senhas de cadeados numéricos etc.;
- processos para autorização e controle de crachás permanentes e provisórios e para áreas seguras ou de acesso restrito:
    - cadastramento de indivíduos;
    - avaliação e aprovação de acesso;
    - emissão, revogação e coleta de crachás;
    - cadastramento e entrega de cartão ou *token* de controle de acesso (RFID de proximidade, gerador de numeração randômica ou similar);
    - cadastramento de *pins* (senhas);
    - cadastramento biométrico etc.;
- processos e rotinas para entrada e saída de equipamentos ou busca e apreensão:
    - registro de entrada e saída de *notebook*, celulares, *tablets* etc.;
    - revista física em bolsas, malas, mochilas etc., de forma geral e impessoal, desde que o procedimento esteja previsto em norma ou regulamento do órgão ou entidade e que tenha sido dada a devida ciência prévia;

- pessoal de vigilância treinado para operação de controle de acesso, incluindo atividades de inspeção visual e tratamento de exceção para o acesso físico.

8.3. Controles de áreas de acesso comum

Os controles de áreas de acesso comum são atividades e mecanismos gerais para o isolamento, a preservação e o bom uso das áreas de acesso geral e comum:

- controladores de acesso (crachás, *pins*, leitores biométricos) nas portas internas e de acesso às escadas;
- segurança em escadas internas de acesso comum;
- segurança em elevadores;
- regras para acesso e uso de ambientes comuns, como restaurantes, enfermarias e salas de descanso;
- regras para acesso e uso de salas de impressora;
- uso de cadeados e controles de travamento de telas para equipamentos desassistidos;
- orientações de mesa limpa (manter o ambiente de trabalho limpo, sem documentos espalhados ou dispositivos móveis e removíveis desprotegidos e à mostra);
- orientações quanto ao acionamento manual de alarmes de emergência (incêndio, alagamento etc.).

8.4. Controles de áreas seguras ou de acesso restrito

Os controles de áreas seguras ou de acesso restrito são atividades e mecanismos adicionais para o isolamento, a preservação e o acesso às áreas críticas e de acesso restrito, tais como:

- CPD;
- salas de monitoramento;
- guaritas de segurança;
- torres de transmissão de dados;
- calhas de cabeamento subterrâneo ou no interior das edificações;
- estações de energia elétrica e geradores;
- estações de tratamento de água e esgoto;
- fossos de elevadores e casas de máquinas;
- almoxarifados e depósitos de equipamentos;
- caixas eletrônicos ou postos bancários etc.

São itens para controle de áreas seguras ou de acesso restrito:

- dispositivos físicos, como catracas, clausuras, leitores de crachá e/ou biométricos, teclados de senha etc.;
- sensores e alarmes;
- câmeras;

- checagem de entrada e saída de equipamentos;
- vigilantes etc.

8.4.1. Identificação de área de acesso restrito

São itens de identificação de área de acesso restrito:

- nome do ambiente;
- nome do responsável;
- forma de contato do responsável;
- localização da área de acesso restrito;
- mapa ou planta da área de acesso restrito;
- tamanho da área de acesso restrito em metros quadrados (m^2);
- lista de pessoas autorizadas a entrar na área de acesso restrito.

8.5. Controles de docas, depósitos e almoxarifados

Os controles de docas, depósitos e almoxarifados são atividades e mecanismos empregados para verificação de entrada e saída de pessoas e materiais em docas, depósitos e almoxarifados.

8.5.1. Identificação de doca, depósito ou almoxarifado

São itens de identificação de doca, depósito ou almoxarifado:

- nome do ambiente;
- nome do responsável;
- forma de contato do responsável;
- localização do ambiente;
- mapa ou planta do ambiente;
- tamanho do ambiente em metros quadrados (m^2);
- lista de pessoas autorizadas a entrar no ambiente.

8.5.2. Recepção em doca, depósito ou almoxarifado

Na recepção de materiais em doca, depósito ou almoxarifado deve-se proceder a:

- registro de:
    - data e hora de chegada do carregamento;
    - local da recepção;
    - empresa de transporte (entrega);
    - responsável pelo transporte (entrega);
    - responsável pela recepção;
    - relação de equipamentos recebidos;
    - detalhamento dos equipamentos recebidos:

        - órgão ou entidade a que pertencem os equipamentos;
        - local de armazenamento temporário dos equipamentos;

- conferência de notas fiscais;
- tratamento de erros e exceções;
- registro de data e hora do término da conferência e recepção do carregamento;
- comunicação da recepção do carregamento para os proprietários.

8.5.3. Despacho em doca, depósito ou almoxarifado

No despacho de materiais em doca, depósito ou almoxarifado deve-se proceder a:

- registro de:
    - data e hora do início do tratamento para despacho;
    - local do despacho;
    - solicitante do despacho;
    - responsável pelo despacho;
    - relação de equipamentos para despacho;
- preparação de equipamentos para despacho;
- registro de detalhamento dos equipamentos despachados:
    - órgão ou entidade a que pertencem os equipamentos;
    - último local de armazenamento dos equipamentos;
- emissão e conferência de notas fiscais de transporte;
- tratamento de erros e exceções;
- registro de data e hora do término da preparação de equipamentos para despacho;
- preenchimento de protocolo de entrega para o transporte:
    - empresa de transporte (retirada);
    - responsável pelo transporte (retirada);
    - data e hora da entrega dos equipamentos para a empresa de transporte;
- comunicação de execução do despacho para o solicitante e para o proprietário, se diferentes.

8.5.4. Controle de correio ou malote

Para controle de correio ou malote deve-se proceder a:

- registro de:
    - data e hora de chegada do pacote e/ou envelope;
    - empresa de transporte (entrega);
    - responsável pelo transporte (entrega);

    - local da recepção;
    - responsável pela recepção;

- atualização da relação de pacotes e envelopes recebidos;
- atualização da relação de destinatários;
- registro de data e hora do encaminhamento para os destinatários;
- preenchimento de protocolo de entrega para o destinatário:

    - responsável pela entrega;
    - data e hora de recepção pelo destinatário;

- atualização do controle de recepção e entrega de pacotes e envelopes.

8.5.5. Controle de almoxarifado e depósito

Para controle de almoxarifado e depósito deve-se:

- seguir as determinações da orientação técnica "Inventário de *hardware* e de *software*", relativa à décima terceira providência da PGDI, no que se refere ao controle periódico dos equipamentos armazenados inclusive em almoxarifados e depósitos;
- controlar a disponibilidade de espaço nos almoxarifados e depósitos para:

    - estimar capacidade de recepção de equipamentos em meses e em volumes com base nos valores médios históricos de entrada e saída de equipamentos;
    - garantir continuidade das atividades de recepção de equipamentos a curto prazo;

- solicitar às áreas proprietárias o encaminhamento ou despacho de equipamentos armazenados e sem uso quando se exceder o tempo de armazenamento originalmente previsto ou o tempo médio de armazenamento;
- solicitar expansão das áreas de armazenamento em caso de esgotamento iminente de capacidade.

8.6. Proteção contra ameaças externas e monitoramento de intrusão

Trata-se dos processos para monitoramento de intrusão (violação de acesso) e proteção contra ameaças externas ou naturais:

- proteção contra ameaças externas e do meio ambiente, incluindo processo para análise, especificação, implantação, operação, manutenção e rotinas para testes de:

    - detectores de fumaça, gás, temperatura, incêndio, umidade, alagamento, poeira;
    - corrimão e guarda-corpo;
    - porta corta-fogo;
    - para-raios, rede elétrica e quadros de energia;
    - hidrantes e extintores;

    - bombas d'água;
    - exaustores de fumaça e gás;
    - geradores de energia, *nobreaks* etc.

- acionamento do time de gestão ou segurança patrimonial em caso de detecção de anomalias ou eventos dessa natureza;
- monitoramento contínuo e vigilância contra violação de acesso, incluindo processo para análise, especificação, implantação, operação, manutenção e rotinas para testes de:

    - portais sensores de RFID;
    - sensores de movimento, ruído ou contato;
    - câmeras de vigilância que cubram:

        - entradas e saídas;
        - rotas, corredores e escadas;
        - muros, alambrados e cercas;
        - áreas externas ou anexas (vizinhas);

    - controladores de rondas de vigilância;
    - alarmes de intrusão, sirenes ou similares;
    - botões de pânico em guaritas ou *halls* de entrada;
    - botão para acionamento manual de alarme de emergência em caso de incêndio, alagamento etc.;
    - sistema de monitoramento e vigilância, como alarmes e CFTV;

- acionamento do time de segurança patrimonial e/ou de gestão de incidentes de segurança da informação em caso de detecção de violação de acesso controlado;
- processo e rotina de testes de evacuação de ambientes;
- relatórios operacionais sobre monitoramento de intrusão e proteção contra ameaças externas;
- recomendações de aplicação de ajustes e melhorias nos controles e processos;
- pessoal treinado para operação de monitoramento de intrusão e execução de ações de proteção contra ameaças externas.

8.7. Outras medidas requeridas pela PGDI

A partir das recomendações elencadas nesta orientação técnica, órgãos e entidades deverão elaborar:

- regras ou critérios adicionais ao estabelecimento de perímetros de segurança para proteção de seus ativos, conforme vigésima segunda providência requerida pela PGDI, em seu Anexo II;

- manual técnico procedimental referente aos procedimentos para segurança física de armazenamento de dados e informações, conforme vigésima quarta providência requerida pela PGDI, em seu Anexo II.