ANEXO IV
NORMA DE SEGURANÇA FÍSICA NO AMBIENTE DE TIC

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução-GP nº 115/2022	

Versionamento:

Versão:	2.0
Data:	22/04/2024
Criada por:	Grupo de Trabalho Técnico (GTT) do CGSI
Aprovada por:	Comitê de Governança de Segurança da Informação (CGSI)
Aprovada em:	22/04/2024

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações
12/06/2023	1.0		
22/04/2024	2.0	GTT do CGSI	Correção da numeração dos tópicos.

1. INTRODUÇÃO

A Norma de Segurança Física no Ambiente de Tecnologia da Informação e Comunicação (TIC) complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para a segurança física dos ativos de TIC críticos do Poder Judiciário do Estado do Maranhão (PJMA).

Para fins desta norma aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I - Glossário da PSI.

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

2. OBJETIVO

Mitigar acesso físico não autorizado, danos e interferências nas informações, ativos e/ou recursos de TIC críticos do PJMA.

3. DIRETRIZES

Orientações da Norma de Segurança Física no Ambiente de TIC.

3.1 Segurança física

Os ativos de TIC críticos serão mantidos em áreas restritas, denominadas áreas restritas de TIC, cujo perímetro é fisicamente protegido contra o acesso não autorizado, danos e quaisquer interferências de origem humana ou natural.

No que se refere ao controle de acesso, circulação e permanência de pessoas nas dependências do PJMA, deverão ser observadas as diretrizes definidas na Resolução-GP nº 115/2022 - TJMA ou posterior que a substitua.

Os crachás de identificação fornecidos pelo PJMA, inclusive provisórios, são pessoais e intransferíveis, não sendo permitido o seu compartilhamento sob nenhuma circunstância.

Quanto à segurança física das área restritas de TIC, deverão ser observadas as seguintes disposições:

I - todo acesso às áreas restritas de TIC deverá, obrigatoriamente, ser autorizado pela DIA, registrando a data e horário de início e fim do acesso para posteriores averiguações em caso de ocorrências;

II - os(as) servidores(as) do PJMA autorizados(as) pela DIA a acessarem as áreas restritas de TIC, deverão portar seus crachás funcionais, fixados em local de fácil visualização;

III - os(as) terceirizados(as), prestadores(as) de serviço e colaboradores(as) registrados(as), após identificação na recepção do prédio sede ou prédios remotos do PJMA, preferencialmente uniformizados(as), portando crachás da empresa, e fixados em local de fácil visualização, deverão ser autorizados(as) pela DIA para acessarem as áreas restritas de TIC do PJMA;

IV - os(as) visitantes registrados(as), devidamente identificados(as) na recepção do prédio sede ou prédios remotos do PJMA, portando crachás provisórios fornecidos pelo PJMA, e fixados em local de fácil visualização, deverão ser autorizados(as) pela DIA para acessarem as áreas restritas de TIC do PJMA;

V - terceirizados(as), prestadores(as) de serviço, colaboradores(as) e visitantes nunca deverão ficar sem acompanhamento ou supervisão nas áreas restritas de TIC do PJMA;

VI - é proibida qualquer tentativa de obtenção ou permissão de acesso de indivíduos(as) não autorizados(as) às áreas restritas de TIC do PJMA;

VII - é resguardado ao PJMA o direito de inspecionar malas, maletas, mochilas, cargas, volumes e similares, assim como quaisquer equipamentos, incluindo dispositivos móveis, antes de permitir a entrada ou saída de terceirizados(as), prestadores(as) de serviço ou colaboradores(as) autorizados(as) a acessar áreas restritas de TIC, incluindo os(as) próprios(as) servidores(as) do PJMA, conforme disposto na Resolução-GP nº 115/2022 - TJMA ou posterior que a substitua;

VIII - é resguardado ao PJMA o direito de, a qualquer momento, abordar pessoas em atitude de fundada suspeita, a fim de realizar procedimentos necessários à vigilância ou à manutenção das áreas restritas de TIC, conforme determinado na Resolução-GP nº 115/2022 - TJMA ou posterior que a substitua;

IX - é resguardado ao PJMA o direito de monitorar as áreas restritas de TIC;

X - não será permitido consumir qualquer tipo de alimento, bebida ou fumar nas áreas restritas de TIC;

XI - armazenar em salas com chave e/ou mobília segura (cofres, armários e gaveteiros com chave) as informações sensíveis das áreas restritas de TIC;

XII - as áreas restritas de TIC deverão conter proteções físicas implementadas contra: incêndio, inundação, umidade, poeira, descarga elétrica, explosão, etc., observando legislações e normativos técnicos vigentes, de acordo com o grau de restrição de cada área;

XIII - as áreas restritas de TIC deverão permanecer livres de quaisquer equipamentos, materiais e/ou objetos que não sejam estritamente necessários à sua finalidade.

Em caso de perda, roubo ou furto de ativos de TIC, sob sua responsabilidade, nas dependências do PJMA, o(a) usuário(a) deverá procurar auxílio das Diretorias Administrativa e de Segurança Institucional e Gabinete Militar para que sejam tomadas as medidas cabíveis, dando ciência para a Diretoria de Informática e Automação através dos canais oficiais de comunicação ou solicitação do PJMA.

4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

4.1 Diretoria de Informática e Automação

É responsabilidade da Diretoria de Informática e Automação:

I - analisar e autorizar solicitações formais de acesso às áreas restritas de TIC do PJMA;

II - gerir e monitorar as instalações físicas das salas de servidores, salas de racks, data centers e salas afins, onde são mantidos os ativos de TIC críticos;

III - manter o registro de acesso, lógico e/ou físico, às áreas restritas de TIC do PJMA;

IV - gerir, monitorar e autorizar o acesso físico de pessoas às áreas restritas de TIC, como salas de servidores, salas de racks, data centers e salas afins, utilizando controles de acesso, tais como biometria, cartões de acesso, senhas, entre outros;

V - realizar testes regulares de segurança física nas áreas restritas de TIC para identificação e mitigação de vulnerabilidades;

VI - treinar e conscientizar os(as) usuários(as) sobre a importância da segurança física nas áreas restritas de TIC, bem como das medidas de proteção adotadas pelo PJMA.

4.2 Diretoria de Segurança Institucional e Gabinete Militar

É competência da Diretoria de Segurança Institucional e Gabinete Militar:

I - gerir sistemas de monitoramento e vigilância, como câmeras de segurança e alarmes, incluindo o alarme de incêndio, para detectar e prevenir intrusões e incidentes de segurança nas áreas restritas de TIC;

II - realizar inspeções regulares para garantir que as portas, janelas e outras entradas físicas das áreas restritas de TIC estejam seguras e em bom estado de conservação e uso;

III - manter registros de acesso físico e lógico para visitantes, fornecedores(as), terceirizados(as), prestadores(as) de serviço ou colaboradores(as) que entram nas dependências do PJMA;

IV - fornecer apoio técnico, por meio de sistema de segurança eletrônica e outros recursos disponíveis, para investigações em andamento de possíveis ilícitos relacionados aos ativos de TIC, incluindo os críticos, mantidos nas áreas restritas de TIC do PJMA.

4.3 Diretoria Administrativa

Compete à Diretoria Administrativa:

I - tomar medidas administrativas a respeito de ativos de TIC (computadores de mesa, impressoras, notebooks, celulares, smartphones, tablets, etc.), dispositivos de armazenamento removível, suportes criptográficos (tokens) e outros ativos de TIC disponibilizados ao(à) usuário(a), que tenham sido objetos de perda, roubo ou furto nas dependências do PJMA.

4.4 Superior Imediato(a) ou Gestor(a) da Unidade Judicial ou Administrativa

Compete ao(à) superior imediato(a) ou gestor(a) da unidade:

I - manter o controle de acesso e guarda das chaves de salas, cofres, armários e gaveteiros, onde estão armazenadas informações sensíveis;

II - solicitar formalmente à DIA, através dos canais oficiais de comunicação ou solicitação do PJMA, a liberação de usuários(as) que necessitam de acesso às áreas restritas de TIC com a devida justificativa.

5. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

6. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

7. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.