PODER JUDICIÁRIO
**JUSTIÇA FEDERAL**
TRIBUNAL REGIONAL FEDERAL - 2ª REGIÃO

# RESOLUÇÃO Nº TRF2-RSP-2023/00043, DE 29 DE NOVEMBRO DE 2023

Dispõe sobre a internalização, no âmbito da Justiça Federal da 2ª Região, da RESOLUÇÃO Nº 687/2020 - CJF, de 15 de dezembro de 2020, que dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2° graus.

O PRESIDENTE DO TRIBUNAL REGIONAL FEDERAL DA 2ª REGIÃO (TRF2), no uso de suas atribuições, RESOLVE:

CONSIDERANDO os termos da RESOLUÇÃO nº 687/2020, do Conselho da Justiça Federal, de 15 de dezembro de 2020;

CONSIDERANDO o deliberado pela Comissão Local de Segurança da Informação (CLSI) em reunião realizada em 08 de agosto de 2023,

RESOLVE:

Art. 1º Internalizar, no âmbito da Justiça Federal da 2ª Região, a Resolução nº 687/2020 - CJF, de 15 de dezembro de 2020 e seus anexos, no que couber.

Art. 2º Os documentos acessórios não comuns ou nacionais serão oficializados por ato do Presidente do Tribunal Regional Federal da 2ª Região, após proposição da Comissão Local de Segurança da Informação – CLSI e aprovação do Presidente do TRF2.

Art. 3º Esta Resolução entra em vigor na data de publicação.

## ANEXO I - Norma de Utilização de Recursos de TI

- **1 Apresentação**

Este é um documento acessório à Política de Segurança da Informação da Justiça Federal que trata da Norma de Utilização de Recursos de TI.

- **2 Escopo**

Esta Norma, bem como os eventuais documentos anexos, tem abrangência regional que inclui o Tribunal Regional Federal da 2ª Região, as Seções Judiciárias do Rio de Janeiro e Espírito Santo, a Escola da Magistratura Regional Federal da 2ª Região – EMARF, o Centro Cultural da Justiça Federal – CCJF e os demais órgãos da Justiça Federal da 2ª Região.

- **3 Público Alvo**

Esta Norma, bem como os eventuais documentos anexos, se aplica a todos os agentes públicos, terceirizados, estagiários, servidores e magistrados da Justiça Federal da 2ª Região.

- **4 Conceituação**

Para efeitos desta Norma considera-se as seguintes conceituações:

- Recurso de TI é todo ou parte de equipamento (hardware) ou programa (software) com tecnologia da informação, bem como qualquer dado acessível por meio desse equipamento ou programa, agregado ou não na forma de estação de trabalho, que integre a qualquer título o patrimônio da Justiça Federal da 2ª Região como ativo tecnológico informático, tangível ou intangível, ou que, mesmo não o integrando, seja utilizado nele ou para ele, o que inclui, dentre outros similares:

- os computadores de mesa (desktops) de qualquer espécie (inclusive os all-in-ones);

- os computadores portáteis (notebooks) de qualquer espécie;

- os computadores portáteis de mão (tablets) de qualquer espécie (inclusive os smartphones);

- os terminais de autoatendimento (quiosques);

- os dispositivos periféricos de qualquer espécie (inclusive para acessibilidade por parte de portadores de necessidades especiais) destinados a conexão em computadores (tais como monitores, teclados, mouses, caixas de som, fones de ouvido, microfones, leitoras, hubs, gravadoras, HDs externos, pen drives, cartões de memória, chips, câmeras, scanners, impressoras, multifuncionais, cartuchos, toners, tokens, smartcards, HSM - hardware security module, equipamentos de biometria, equipamentos de videoconferência, projetores, touch boards, mesas digitalizadoras, modems, roteadores, cabos, adaptadores, estabilizadores, filtros e no-breaks);

- os equipamentos que compõem o data center;

- os equipamentos de redes internas, bem como a rede de comunicação de dados que as interliga e as liga a redes externas (Internet), com ou sem fio (via onda infravermelha, Wi-Fi, Bluetooth, outras espécies de ondas de rádio etc.);

- os programas de computador de qualquer espécie (tais como aplicativos e sistemas);

- os endereços e correios eletrônicos (tais como sites, e-mails, calendários, agendas, catálogos de contatos e gerenciadores de tarefas);

- as ferramentas eletrônicas de comunicação de dados de qualquer espécie;

- os dados de qualquer espécie armazenados em computadores, dispositivos periféricos e outros equipamentos, bem como em CDs, DVDs e outras mídias, dispostos ou não em banco de dados (tais como arquivos e certificados digitais).

- AUTENTICIDADE - propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
- CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;
- CRIPTOGRAFIA: técnica para proteção da informação, através da codificação dos dados com uso de chave e procedimento algoritmo, permitindo acesso aos dados somente ao(s) possuidor(es) da chave.
- DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;
- ESTAÇÃO DE TRABALHO: microcomputador (com periféricos como monitor, mouse e teclado) ou notebook institucional.
- INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- PRIVILÉGIO MÍNIMO: princípio de que um usuário precisa acessar os sistemas somente com os recursos mínimos necessários para realizar suas atividades.

- **5 Objetivos**

Os objetivos desta Norma são, essencialmente, regulamentar a utilização dos recursos de tecnologia da informação com seus requisitos de segurança (ou seja, confidencialidade, integridade, disponibilidade e autenticidade), levando em consideração as vulnerabilidades exploráveis por ameaças e agressões com risco de impacto negativo, e tendo ênfase no aspecto da segurança física, descrita no item 2.1 do Anexo II da Resolução nº 687, de 15 de dezembro de 2020, do CJF.

Esta Norma é complementada pelos demais documentos acessórios à Política de Segurança da Informação da Justiça Federal, com ênfase em outros aspectos.

- **6 Documentos de Referência**

Os documentos de referência desta Norma são, principalmente, os seguintes:

- Art. 38 da Resolução nº 370, de 28 de janeiro de 2021, do CNJ;
- Art. 1º, §§ 1º e 2º da Resolução nº 435, de 28 de outubro de 2021;

- Anexo da Resolução nº 91, de 29 de setembro de 2009, do CNJ;
- "Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário" elaboradas pelo Comitê Nacional de Gestão de Tecnologia da Informação e Comunicação do Poder Judiciário;
- Boas práticas em segurança da informação / Tribunal de Contas da União. – 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.
- Resolução nº 22, de 30 de maio de 2011, do Tribunal Regional Federal da 2ª Região; (alterada pela Resolução TRF2-RSP-2019/00077)
- Anexo da Portaria nº 124, de 10 de abril de 2013, do CJF.
- Além desses, os documentos de referência desta Norma são, essencialmente, os seguintes:
- Lei nº 12.682, de 9 de julho de 2012; (Alterada pela Lei 13.874/2019)
- Arts. 3º, caput, VI, 4º, caput, VIII, e 10, caput, II, da Resolução nº 182, de 17 de outubro de 2013, do CNJ;
- Orientação nº 3, de 5 de março de 2007, da Corregedoria Nacional de Justiça;
- Instrução Normativa nº 24-14, de 30 de setembro de 2008, do Tribunal Regional Federal da 2ª Região.

- **7 Disposições Gerais**

7.1 **Dos usuários dos recursos de TI**

- Poderá ser usuário dos recursos de TI todo o público-alvo desta Norma, definido no item 3 da mesma, sendo necessário, com sua concordância tácita ou expressa, de qualquer forma, o respectivo termo de responsabilidade, conforme a Política de Segurança da Informação implantada no âmbito da Justiça Federal da 2ª Região.

**7.2 Dos recursos de TI passíveis de utilização**

7.2.1Para integrarem ou deixarem de integrar a qualquer título o patrimônio da Justiça Federal da 2ª Região, bem como para terem expandida sua utilização, os recursos de TI deverão se submeter previamente, conforme o caso, a:

- contratação;
- teste, avaliação e homologação, pela unidade responsável pela TI, em conjunto com o respectivo GN, com ênfase nos requisitos de segurança da informação, principalmente o nível de impacto negativo; e
- autorização ou aprovação, pela Presidência, com assessoramento por parte da CLSI, com ênfase nos mesmos requisitos.

7.2.2 Deverão ser utilizados na Justiça Federal da 2ª Região ou para ela os recursos de TI que integrem a qualquer título seu patrimônio.

7.2.3 Também poderão ser utilizados na Justiça Federal da 2ª Região ou para ela, excepcionalmente, os recursos de TI que não integrem seu patrimônio, inclusive na linha do "BYOD - Bring Your Own Device" (ou seja, "traga seu próprio dispositivo") ou da computação em nuvem (cloud computing), principalmente em situações de contingência, desde que previamente submetidos, conforme o caso, às operações descritas no item 7.2.1 desta Norma.

7.2.4 Os recursos de TI deverão ser agregados na forma de estações de trabalho conforme um padrão comum, para a grande maioria das unidades e usuários, que exerce atividades sem peculiaridades técnicas, ou conforme determinados padrões especiais (tais como para administradores, técnicos, designers, editores, estagiários,

empregados de "terceirizados", magistrados, advogados, inspetores, auditores, ou para acessibilidade por parte de portadores de necessidades especiais), observando o princípio do privilégio mínimo.

7.2.5 Os usuários devem contribuir para o adequado funcionamento e segurança dos recursos de TI da Justiça Federal da 2ª Região, sendo responsáveis pelos recursos de tecnologia da informação de utilização própria.

7.2.6 A área de Tecnologia da Informação deverá manter lista atualizada de hardwares e softwares homologados que poderão ser utilizados no ambiente da Justiça Federal da 2ª Região observando o princípio do privilégio mínimo.

7.2.7 É vedada a utilização de hardwares e softwares que não estejam previamente autorizados, licenciados e homologados.

7.2.8 É vedada a gravação de arquivos (música, fotos, vídeos e outros), que não estejam estritamente relacionados às atividades funcionais, nos servidores e sistemas de armazenamento centralizados/corporativos da Justiça Federal da 2ª Região.

7.2.9 A área de Tecnologia da Informação poderá proceder à desinstalação de hardwares e softwares e à eliminação de arquivos que estejam em desacordo com o presente ato normativo, autorizada pelo Presidente, no âmbito da Justiça Federal da 2ª Região, Diretor do Foro, no âmbito da Seção Judiciária, ou por servidor com delegação para tanto.

7.2.10 O deslocamento de qualquer recurso de Tecnologia da Informação, na unidade ou entre unidades, deve ser comunicado pelo detentor da carga à área responsável pelo controle de patrimônio, a fim de que seja registrada a ocorrência.

7.2.11 Os conteúdos e práticas dos recursos de TI não poderão comprometer o desempenho técnico dos próprios recursos, bem como o desempenho nas atividades funcionais de seu usuário.

**7.3 Das finalidades dos recursos de TI**

7.3.1 Os recursos de TI, disponibilizados às diversas áreas da Justiça Federal da 2ª Região, destinam-se, exclusivamente, ao atendimento das necessidades do serviço público, sendo vedada a utilização para fins particulares.

**7.4 Dos conteúdos dos recursos de TI**

7.4.1 Os recursos de TI, com destaque para os computadores, impressoras, softwares e arquivos, deverão tratar de informações necessárias ou úteis ao serviço prestado na Justiça Federal da 2ª Região.

7.4.2 Eventualmente, os recursos de TI também poderão tratar de informações que, embora não sejam necessárias ou úteis ao serviço prestado na Justiça Federal da 2ª Região, sejam concernentes à serviços públicos ou temas de interesse público, governo e outros poderes estatais.

7.4.3 Os recursos de TI não poderão tratar de informações ilícitas, abusivas ou com alto risco de impacto negativo, constatado pela unidade responsável pela TI, bem

como que sejam concernentes a temas muito distantes dos descritos no item 7.4.2 desta Norma, enquanto desnecessárias ou inúteis ao serviço público, o que inclui, dentre outros similares:

- conteúdos que sejam objeto de crime, contravenção, improbidade administrativa, infração disciplinar ou ética, ato jurídico ilícito ou qualquer outra espécie de infração;
- pornografia;
- violência;
- assuntos pessoais, inclusive relacionamentos;
- jogos e qualquer outra espécie de entretenimento.

7.4.4 São passíveis de auditoria quaisquer informações geradas, recebidas, processadas ou armazenadas utilizando os recursos de TI da Justiça Federal da 2ª Região.

7.4.5 A área de Tecnologia da Informação não é responsável pela salvaguarda das informações armazenadas em local que não esteja em conformidade com a Política de Segurança.

**7.5 Das práticas com os recursos de TI**

7.5.1 Os recursos de TI, com destaque para os computadores, impressoras, softwares e arquivos, deverão tratar de informações necessárias ou úteis ao serviço prestado na Justiça Federal da 2ª Região.

7.5.2 Eventualmente, os recursos de TI também poderão tratar de informações que, embora não sejam necessárias ou úteis ao serviço prestado na Justiça Federal da 2ª Região, sejam concernentes à serviços públicos ou temas de interesse público, governo e outros poderes estatais.

7.5.3 Os recursos de TI não poderão ser aplicados de modo ilícito, abusivo ou com alto risco de impacto negativo, constatado pela unidade responsável pela TI, bem como que sejam concernentes a temas muito distantes dos descritos no item 7.5.2 desta Norma, enquanto desnecessárias ou inúteis ao serviço público, o que inclui, dentre outros similares:

- práticas que configurem crime, contravenção ou qualquer outra espécie de infração;
- interceptação, invasão, subtração, adulteração, prejuízo ou destruição de recursos de TI, mediante violação ou desativação de mecanismos de controle de segurança da informação (hacking);
- proliferação de softwares maliciosos (malwares) ou exploradores de vulnerabilidades (exploits) de qualquer espécie (tais como vírus, worms, "Cavalos de Tróia" e keyloggers);
- obtenção de informações mediante fraude ("phishing"), ou de qualquer outra espécie de vantagem mediante fraude, num contexto de "engenharia social";
- difusão de informações de qualquer espécie (texto, imagem estática, imagem dinâmica ou som) não solicitadas ("SPAM - sending and posting advertisement in mass", ou seja, "enviar e postar publicidade em massa"), principalmente com caráter comercial, político, partidário, eleitoral etc.;
- difusão de notícias falsas (“fake news”) e boatos ("hoaxes");
- difusão de correntes.

7.5.4 Os dados deverão ser armazenados, conforme os níveis de acesso, criticidade ou prioridade, em dispositivos:

- apropriados;
- com limite de capacidade adequado;
- preferencialmente internos, inclusive, se for o caso, com segregação ("conteinerização");
- preferencialmente estatais;
- com criptografia baseada em algoritmo de Estado.

7.5.5 Os dados também poderão ser armazenados, excepcionalmente, conforme os níveis de acesso, criticidade ou prioridade, em dispositivos:

- externos;
- particulares, individuais ou compartilháveis;
- sem criptografia.

7.5.6 Todos os dados armazenados, com destaque para os críticos ou prioritários, deverão ou poderão ter cópias de segurança (backups) providenciadas, periodicamente, por seu proprietário, possuidor ou detentor, conforme o caso.

7.5.7 Os recursos de TI que integrem o patrimônio da Justiça Federal da 2ª Região poderão ser utilizados, excepcionalmente, fora de suas instalações, independentemente de ser ou não em tele trabalho, principalmente em situações de contingência, desde que previamente submetidos, conforme o caso, às operações descritas no item 7.2.1 desta Norma.

7.5.8 Se vierem a estar fora da vigilância de seu proprietário, possuidor ou detentor, inclusive em trânsito, independentemente de estar sendo utilizado em tele trabalho, bem como se vierem a deixar de ser utilizados, o computador, bem como todas as específicas formas de acesso lógico, deverão se submeter a desligamento, bloqueio ou saída (sign-out, logoff ou logout), preferencialmente de modo automático.

7.5.9 É recomendável que o computador portátil disponha de mecanismos remotos de localização via rede ou GPS, bem como de desligamento, bloqueios, saída (logoff ou logout), cópia de segurança (backup) e apagamento, preferencialmente de modo automático.

7.5.10 O documento impresso que tiver sido definido como controlado, e, assim, que contiver informação classificada em qualquer grau de sigilo, conforme a Lei nº 12.527, de 18 de novembro de 2011, ou em qualquer grau de limitação equivalente, caso a pertinente tecnologia e processos de trabalho adotados no Tribunal ainda não estejam ajustados a essa lei, deverá ser imediatamente recolhido da bandeja de saída da impressora compartilhada, bem como fragmentado ou devidamente rasurado, caso se trate de documento inutilizável, não obstante o art. 15 da Resolução nº 23, de 19 de setembro de 2008, do CJF.

### 7.6 Do controle da utilização dos recursos de TI

7.6.1 O controle da utilização de recursos de TI, pela unidade responsável pela TI:

- poderá ser preventivo, detectivo ou reativo, dando-se prévia, simultânea ou posteriormente, priorizando-se o primeiro;
- deverá ser previamente avisado e agendado, exceto se for alto o risco de impacto negativo, constatado pela unidade responsável pela TI;

- poderá ser ordinário ou extraordinário, gerando relatório.

7.6.2 Poderão ser utilizados os seguintes mecanismos de controle:

- efetuação de registro (tal como tombamento) e manutenção preferencialmente durante o prazo para aplicar ou buscar a aplicação da penalidade para o tipo de infração mais grave;
- rastreamento, varredura ou verificação periódica (tal como levantamento físico e inventário);
- bloqueio de conteúdo;
- limitação de prática;
- restrição de propriedades (tais como tipo e tamanho);
- submissão a quarentena ou suspensão;
- remoção ou interrupção;
- inspeção periódica.

7.6.3 Os mecanismos de controle, sempre atualizados, deverão ser ativados de modo automatizado (tal como mediante a utilização de software anti-vírus e anti-malware), sem a possibilidade de desativação, ressalvada a possibilidade de revisão do resultado dessa automatização, a pedido ou de ofício, pelo GN; e resguardada a inviolabilidade do sigilo dos dados classificados em qualquer grau de sigilo, conforme a Lei nº 12.527, de 2011, ou em qualquer grau de limitação equivalente, caso a pertinente tecnologia e processos de trabalho adotados no Tribunal ainda não estejam ajustados a essa lei.

7.6.4 De modo complementar, os arquivos armazenados em dispositivos apropriados, quando abertos pela primeira vez, deverão se submeter a utilização de software antivírus.

7.6.5 Aplicam-se subsidiariamente os mecanismos de controle de todos os recursos materiais.

7.6.6 Qualquer incidente que, envolvendo utilização de recursos de TI, aparentemente tenha relevante risco de impacto negativo, deverá ser imediatamente reportado, por quem tomar conhecimento, ou mesmo de modo automatizado, ao respectivo GN e, daí, à CLRI, para os devidos fins.

- **8 Disposições Finais**

Os gestores de negócio deverão providenciar a implantação da Norma de Segurança de Acesso Físico e Ambiental bem como os registros e a divulgação das informações de que trata esta norma.

## ANEXO II - Norma de Segurança de Acesso Lógico

### 1 Apresentação

Este é um documento acessório à Política de Segurança da Informação da Justiça Federal que trata da Norma de Segurança de Acesso Lógico aos ativos de informação.

### 2 Escopo

Esta Norma, bem como os eventuais documentos anexos, tem abrangência regional que inclui o Tribunal Regional Federal da 2ª Região, as Seções Judiciárias do Rio de Janeiro e Espírito Santo, a Escola da Magistratura Regional Federal da 2ª Região – EMARF, o Centro Cultural da Justiça Federal – CCJF e os demais órgãos da Justiça Federal da 2ª Região.

### 3 Público Alvo

Esta Norma, bem como os eventuais documentos anexos, se aplica a todos os agentes públicos, terceirizados, estagiários, servidores e magistrados da Justiça Federal da 2ª Região.

### 4 Conceituação

Para efeitos desta Norma, considera-se acesso lógico toda forma de ingresso (sign-in, login ou logon), circulação, permanência, utilização e saída (sign-out, logoff ou logout) de computadores, aplicativos, sistemas, sites e e-mails, presentes em redes internas (Intranet), virtualmente internas (seja VNC - virtual network computing ou VPN - virtual private network) ou externas (Internet), conectadas com ou sem fio, e com ou sem o intermédio de ferramenta eletrônica de comunicação de dados de qualquer espécie, que integre a qualquer título o patrimônio da Justiça Federal da 2ª Região como ativo tecnológico informático, tangível ou intangível, ou que, mesmo não o integrando, seja utilizado nela ou para ela.

### 5 Objetivos

Os objetivos desta Norma são, essencialmente, assegurar os simultâneos acessos e proteção da informação com seus principais requisitos de segurança (ou seja, confidencialidade, integridade, disponibilidade e autenticidade), levando em consideração as vulnerabilidades exploráveis por ameaças e agressões com risco de impacto negativo, e tendo ênfase no aspecto da segurança física, descrita no item 2.1 do Anexo II da Resolução nº 687, de 15 de dezembro de 2020, do CJF.

Esta Norma é complementada pelos demais documentos acessórios à Política de Segurança da Informação da Justiça Federal, com ênfase em outros aspectos.

### 6 Documentos de Referência

Os documentos de referência desta Norma são, principalmente, os seguintes:

- Art. 38 da Resolução nº 370, de 28 de janeiro de 2021, do CNJ;
- Art. 1º, §§ 1º e 2º da Resolução nº 435, de 28 de outubro de 2021;

- Anexo da Resolução nº 91, de 29 de setembro de 2009, do CNJ;
- "Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário" elaboradas pelo Comitê Nacional de Gestão de Tecnologia da Informação e Comunicação do Poder Judiciário;
- Boas práticas em segurança da informação / Tribunal de Contas da União. – 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.
- Resolução nº 22, de 30 de maio de 2011, do Tribunal Regional Federal da 2ª Região; (alterada pela Resolução TRF2-RSP-2019/00077)
- Anexo da Portaria nº 124, de 10 de abril de 2013, do CJF;
- Além desses, os documentos de referência desta Norma são, essencialmente, os seguintes:
- Lei nº 12.682, de 9 de julho de 2012; (Alterada pela Lei 13.874/2019)
- Arts. 3º, caput, VI, 4º, caput, VIII, e 10, caput, II, da Resolução nº 182, de 17 de outubro de 2013, do CNJ;
- Orientação nº 3, de 5 de março de 2007, da Corregedoria Nacional de Justiça;
- Instrução Normativa nº 24-14, de 30 de setembro de 2008, do Tribunal Regional Federal da 2ª Região;

## 7 Disposições Gerais

### 7.1 Dos que podem ter acesso lógico

7.1.1 Poderá ter acesso lógico todo o público-alvo desta Norma, definido no item 3 da mesma, sendo necessária sua concordância tácita ou expressa, de qualquer forma, à Política de Segurança da Informação implantada no âmbito da Justiça Federal da 2ª Região.

### 7.2 Do acesso lógico passível de concessão

7.2.1 Para integrarem a qualquer título o patrimônio da Justiça Federal da 2ª Região, bem como para terem expandida sua utilização, as formas de acesso lógico deverão se submeter previamente, conforme o caso, a:

- Contratação;
- Teste, avaliação e homologação, pela unidade responsável pela TI, em conjunto com o respectivo GN, com ênfase nos requisitos de segurança da informação, principalmente o nível de impacto negativo;
- Autorização ou aprovação, pela Presidência, com assessoramento por parte da CLSI, com ênfase nos mesmos requisitos.

7.2.2 Deverão ser utilizadas na Justiça Federal da 2ª Região ou para ela as formas de acesso lógico que integrem a qualquer título seu patrimônio.

7.2.3 Também poderão ser utilizadas na Justiça Federal da 2ª Região ou para ela, excepcionalmente, as formas de acesso lógico que não integrem seu patrimônio, inclusive na linha do "BYOD - bring your own device" (ou seja, "traga seu próprio dispositivo") ou da computação em nuvem (cloud computing), principalmente em situações de contingência, desde que previamente submetidos, conforme o caso, às operações descritas no item 7.2.1 desta Política Norma.

7.2.4 Os computadores que não integrem o patrimônio da Justiça Federal da 2ª Região poderão estar presentes em redes internas apenas se conectados sem fio, ou com fio, situação em que deverão ter configuração idêntica à previamente estabelecida para as estações de trabalho institucionais.

7.2.5 O acesso lógico deverá se dar a partir da prévia autorização ao serviço, sucedida, preferencialmente, pela concomitante autenticação do usuário.

7.2.6 A autorização ao serviço deverá se dar por meio da concessão, pelo GN, de permissão ao usuário ou grupo, para agir de determinadas maneiras (tais como ler, modificar etc.), conforme a anterior definição, também pelo GN, dos diferentes perfis, baseados na forma de vínculo, atribuições, unidade ou níveis de acesso, criticidade ou prioridade da informação.

7.2.7 A permissão deverá ser individual e intransferível, sendo possíveis, no entanto, a herança de permissão e o regime de expressa substituição eventual.

7.2.8 Como preceito geral, deverão ser definidos um perfil comum com mínimo privilégio, para a grande maioria das unidades e usuários, que exerce atividades sem peculiaridades técnicas relevantes, e determinados perfis especiais (tais como para administradores, técnicos, *designers*, editores, estagiários, empregados de "terceirizados", magistrados, advogados, inspetores e auditores) com privilégio compatível, para as unidades e usuários que exercem atividades com peculiaridades técnicas relevantes.

7.2.9 O administrador deverá ter a possibilidade de modular entre o perfil comum e o perfil especial para administradores, estritamente conforme a ação pretendida.

7.2.10 Todas as formas de acesso lógico deverão ter uma configuração previamente estabelecida pela unidade responsável pela TI, principalmente quanto aos processos técnicos passíveis de automação (tais como os que envolvem cookie, script, plug-in, pop-up, download, upload, macro, notificação etc.), ressalvada a possibilidade de ajustes de menor risco e impacto por parte do próprio usuário.

7.2.11 A autenticação do usuário deverá se dar por meio de sua identificação, conforme seu anterior credenciamento (sign-up), pelo GN, em ACL - access control list (ou seja, lista de controle de acesso), na forma de conta de serviços, baseada na credencial completa, composta:

- pelo que se sabe em termos de informação (tal como identidade, senha, dados pessoais etc.); e
- pelo que se tem em termos de tecnologia (tal como token, smartcard etc.); ou
- pelo que se é em termos de características biométricas (tal como mediante impressão digital, impressão palmar, caligrafia, formação da íris, voz, perfil genético etc.).

7.2.12 A credencial deverá ser individual e intransferível.

7.2.13 Não poderá existir conta de serviços genérica ou compartilhada, exceto se houver outro modo de identificação do usuário, bem como se for baixo o risco de impacto negativo, constatado pelo GN.

7.2.14 Sempre que tecnicamente possível:

- O credenciamento (sign-up) deverá compartilhar dados com o registro de incidentes de segurança da informação.
- A autenticação do usuário deverá ser acompanhada da transcrição de caracteres de imagem dinâmica com geração automática ("CAPTCHA - Completely

Automated Public Turing Test to Tell Computers and Humans Apart"), em razão de tentativa errônea de autenticação do usuário;
- A autenticação do usuário deverá ser forte, enquanto baseada na credencial completa e limitada quanto a número de sucessivas tentativas;
- A autenticação do usuário não poderá ser automática ou se submeter a preenchimento automático em formulário;
- A conta de serviços deverá ter um prazo de validade, conforme a forma de vínculo ou as atividades exercidas;
- A conta de serviços deverá ser suspensa ou interrompida, em razão de sucessivas tentativas errôneas de autenticação do usuário ou inatividade trimestral;
- A identidade, a senha e os dados pessoais verificados na forma de perguntas e respostas deverão se submeter a padronização quanto a serviço a que são destinados, tamanho mínimo e máximo em número de caracteres, formato em tipos de caracteres e efeitos, e periodicidade de efetiva troca, sem prejuízo dos dados pessoais utilizados apenas para lembrar a senha;
- A geração, entrega e alteração da senha deverão se dar de modo a garantir a manutenção do respectivo sigilo.
- A senha deverá ser forte, enquanto dotada de muitos caracteres de todos os tipos (alfanumérica), em caixa alta e baixa, não idêntica à eventualmente anterior, difícil de adivinhar, e sujeita a efetiva troca no mínimo semestral, principalmente para as formas de acesso lógico que envolvem alto risco de impacto negativo, constatado pela unidade responsável pela TI;
- A senha para o primeiro ingresso (sign-in, login ou logon) deverá ter um prazo de expiração;
- A senha preenchida em formulário deverá ser invisível e, para acessibilidade por parte de portadores de necessidades especiais de audição, não poderá ser falada;
- A senha deverá se submeter a imediata e efetiva alteração no primeiro ingresso (sign-in, login ou logon), bem como quando houver anormalidade quanto à permissão ou credencial, ou suspeita de perda do respectivo sigilo, sem prejuízo da efetiva troca periódica;
- A sessão da específica forma de acesso lógico deverá ter um prazo de expiração (time-out).

7.2.15 As finalidades, conteúdos e práticas de acesso lógico não poderão comprometer o desempenho técnico dos computadores, aplicativos, sistemas, sites, e-mails e redes, bem como o desempenho funcional de seu usuário, se for o caso.

7.2.16 Qualquer conduta deverá ter sua relevância avaliada independentemente de ser comissiva ou omissiva, dolosa ou culposa, consumada ou tentada.

**7.3 Das finalidades do acesso lógico**

7.3.1 O acesso lógico deverá se dar em atividades imediatamente relacionadas ao serviço prestado na Justiça Federal da 2ª Região, por lhe serem necessárias, e poderá se dar em atividades mediatamente relacionadas ao serviço nela prestado, por lhe serem úteis.

7.3.2 O acesso lógico também poderá se dar em atividades não relacionadas ao serviço prestado na Justiça Federal da 2ª Região, desde que configurem práticas autorizadas.

**7.4 Dos conteúdos passíveis de acesso lógico**

7.4.1 O acesso lógico, com destaque para os computadores, aplicativos, sistemas, sites, e-mails e redes, deverá se dar para tratar de informações necessárias ou úteis ao serviço prestado na Justiça Federal da 2ª Região.

7.4.2 O acesso lógico também poderá se dar para tratar de informações que, embora não sejam necessárias ou úteis ao serviço prestado na Justiça Federal da 2ª Região, sejam concernentes, dentre outros temas, a educação, saúde, trabalho, comunicação, cidadania, serviços públicos ou de interesse público, governo e poderes estatais, o que inclui, dentre outros correlatos:

- instituições de ensino ou pesquisa;
- planos de saúde;
- entidades sindicais ou associativas;
- meios de comunicação social;
- transporte e trânsito;
- segurança;
- previsão do tempo;
- provedores de e-mails não institucionais;
- blogs, redes e mídias sociais profissionais ou institucionais estatais;
- páginas, perfis e canais institucionais estatais em redes ou mídias sociais.

7.4.3 O acesso lógico não poderá se dar para tratar de informações ilícitas, imorais, abusivas, inconfiáveis, inseguras, anônimas ou com alto risco de impacto negativo, constatado pela unidade responsável pela TI, bem como que sejam concernentes a temas muito distantes dos descritos no item 7.4.2 desta Norma, enquanto desnecessárias ou inúteis ao serviço prestado na Justiça Federal da 2ª Região, o que inclui, dentre outros similares:

- pornografia;
- violência;
- assuntos pessoais, inclusive relacionamentos;
- jogos e qualquer outra espécie de entretenimento;
- concursos de prognósticos (tais como sorteios, loterias e apostas);
- salas de bate-papo (chat) não profissionais;
- páginas, perfis e canais não institucionais estatais em blogs, redes ou mídias sociais.

### 7.5 Das práticas de acesso lógico

7.5.1 O acesso lógico não poderá se dar de modo ilícito, imoral, abusivo, inconfiável, inseguro, anônimo ou com alto risco de impacto negativo, constatado pela unidade responsável pela TI, o que inclui, dentre outros similares:

- Interceptação, invasão, subtração, adulteração, prejuízo ou destruição de informações ou formas de acesso lógico, mediante violação ou desativação de mecanismos de controle de segurança da informação.
- Proliferação de softwares maliciosos (malwares) ou exploradores de vulnerabilidades (exploits) de qualquer espécie (tais como vírus, worms, "Cavalos de Tróia" e keyloggers);
- Obtenção de informações mediante fraude ("phishing"), ou de qualquer outra espécie de vantagem mediante fraude, num contexto de "engenharia social";
- Adulteração de site (cracking, defacement ou "pichação");
- Congestionamento ou derrubada de formas de acesso lógico mediante ação em massa de qualquer espécie (DOS, DDOS, Brute Force,...)

- Difusão de informação institucional falsa;
- Difusão de informações de qualquer espécie (texto, imagem estática, imagem dinâmica ou som) não solicitadas ("SPAM - sending and posting advertisement in mass"), principalmente com caráter comercial, político, partidário, eleitoral etc.;
- Difusão de boatos ("hoaxes");
- Difusão de correntes;
- Utilização de serviço proxy

7.5.2 Sempre que tecnicamente possível, todo documento criado por meio de específica forma de acesso lógico deverá ter assinatura eletrônica.

7.5.3 Os dados deverão preferencialmente trafegar, conforme os níveis de acesso, criticidade ou prioridade, em canais apropriados, com limite de capacidade adequado, preferencialmente interno ou estatais, e com criptografia baseada em algoritmo de Estado.

7.5.4 Se vierem a estar fora da vigilância de seu proprietário, possuidor ou detentor, inclusive em trânsito, independentemente de estar sendo utilizado em teletrabalho, bem como se vierem a deixar de ser utilizados, o computador, bem como todas as específicas formas de acesso lógico, deverão se submeter a desligamento, bloqueio ou saída (sign-out, logoff ou logout), preferencialmente de modo automático.

**7.6 Do efetivo controle de acesso lógico**

7.6.1 O efetivo controle de acesso lógico, pela unidade responsável pela TI:

- poderá ser preventivo, detectivo ou reativo, dando-se prévia, simultânea ou posteriormente, priorizando-se o primeiro;
- poderá ser ordinário ou extraordinário, gerando relatório periódico.

7.6.2 Poderão ser utilizados os seguintes mecanismos de efetivo controle:

- efetuação de registros (tais como log) e manutenção preferencialmente durante o prazo para aplicar ou buscar a aplicação da penalidade para o tipo de infração mais grave;
- monitoramento de tráfego constante (tal como mediante sniffer);
- rastreamento, varredura ou verificação periódica;
- implantação de filtro (firewall);
- implantação de sensores, bem como de alertas sonoros e visuais, com funcionamento constante;
- realização de teste (tal como pentest, inclusive mediante honeypot ou honeynet) periódico;
- bloqueio de conteúdo;
- limitação de prática;
- restrição de propriedades (tais como tipo e tamanho);
- submissão a quarentena ou suspensão;
- invalidade ou expiração;
- remoção ou interrupção;
- inspeção periódica

7.6.3 Os mecanismos de efetivo controle, sempre atualizados, deverão ser ativados de modo automatizado (tal como mediante a utilização de software antivírus),

sem a possibilidade de desativação, ressalvada a possibilidade de revisão do resultado dessa automatização, a pedido ou de ofício, pelo GN; e resguardada a inviolabilidade do sigilo das informações pessoais, sensíveis ou sigilosas.

7.6.4 A inviolabilidade referida no item 7.6.3 desta Norma não impede a coleta, uso, armazenamento e tratamento de registros estritamente para o fim de manutenção preventiva, adaptativa, evolutiva ou corretiva.

7.6.5 De modo complementar, os arquivos recebidos por meio de acesso lógico, quando abertos pela primeira vez, deverão se submeter a utilização de software antivírus.

7.6.6 Aplicam-se subsidiariamente o processo de gestão de riscos e o Catálogo de Fraudes do CAIS - Centro de Atendimento a Incidentes de Segurança da RNP (Rede Nacional de Ensino e Pesquisa).

7.6.7 Qualquer incidente que, envolvendo acesso lógico, aparentemente tenha relevante risco de impacto negativo, deverá ser imediatamente reportado, por quem tomar conhecimento, ou mesmo de modo automatizado, ao respectivo GN e, daí, à CLRI, para os devidos fins.

**8 Disposições Finais**

Os gestores de negócio deverão providenciar a implantação da Norma de Segurança de Acesso Físico e Ambiental bem como os registros e a divulgação das informações de que trata esta norma.

## ANEXO III - Norma de Segurança de Acesso Físico e Ambiental

### 1 Apresentação

Este é um documento acessório à Política de Segurança da Informação da Justiça Federal que trata da Norma de Segurança de Acesso Físico e Ambiental às instalações envolvidas na guarda de dados e informações.

Estabelece as regras básicas necessárias ao controle de acesso físico e ambiental às instalações envolvidas na guarda de dados e informações, para prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento de dados e informações e nas informações da organização. Aborda também os aspectos relacionados com a monitoração do ambiente, incluindo climatização e proteção elétrica.

### 2 Escopo

Esta Norma, bem como os eventuais documentos anexos, tem abrangência regional que inclui o Tribunal Regional Federal da 2ª Região, as Seções Judiciárias do Rio de Janeiro e Espírito Santo, a Escola da Magistratura Regional Federal da 2ª Região – EMARF, o Centro Cultural da Justiça Federal – CCJF e os demais órgãos da Justiça Federal da 2ª Região.

### 3 Público Alvo

Esta Norma, bem como os eventuais documentos anexos, se aplica a todos os agentes públicos, terceirizados, estagiários, servidores e magistrados da Justiça Federal da 2ª Região.

### 4 Conceituação

Para efeitos desta Norma, considera-se acesso físico às instalações envolvidas na guarda dos dados e informações o ingresso, circulação, permanência ou saída de arquivos, sala-cofre, unidades processantes e de protocolo, gabinetes de magistrados, salas de trabalho, centrais telefônicas, salas de automação, unidades responsáveis por fonografia e taquigrafia, segurança institucional, saúde, acompanhamento de bens e rendas particulares, processos disciplinares, concursos públicos, licitações e processos criativos, dentre outras similares.

Por sua vez, considera-se segurança de acesso ambiental as medidas de segurança adotadas no ambiente físico da organização, onde estão contidos ou pretende-se disponibilizar acessos a ativos de informações. Isso inclui a adoção de medidas de segurança preventiva com o intuito de prevenir danos ambientais causados por incêndios, inundações, desmoronamentos etc; bem como aspectos relacionados com a monitoração do ambiente, incluindo climatização e proteção elétrica. Visa a proteção física de pessoas, bens e instalações contra danos físicos causados por sinistros naturais ou de causas não intencionas e também as intencionais/criminosas.

### 5 Objetivos

Os objetivos desta Norma são, essencialmente, assegurar os simultâneos acessos e proteção da informação com seus principais requisitos de segurança como a confidencialidade, integridade, disponibilidade e autenticidade, levando em consideração as vulnerabilidades exploráveis por ameaças e agressões com risco de impacto negativo,

com ênfase no aspecto da segurança física e ambiental, descrita no item 2.1 do Anexo II da Resolução nº 687, de 15 de dezembro de 2020, do CJF.

Esta Norma é complementada pelos demais documentos acessórios à Política de Segurança da Informação da Justiça Federal, com ênfase em outros aspectos.

**6 Documentos de Referência**

Alguns documentos de referência desta Norma:

Resolução nº 370, de 28 de janeiro de 2021, do CNJ;

Resolução nº 435, de 28 de outubro de 2021, do CNJ;

Resolução nº 687, de 15 de dezembro de 2020, do CJF;

Resolução nº 91, de 29 de setembro de 2009, do CNJ;

Resolução nº TRF2-RSP-2019/00077, de 30 de setembro de 2019, do TRF2;

Resolução nº TRF2-RSP-2019/00046, de 24 de junho de 2019 do TRF2;

Lei nº 13.874, de 20 de setembro de 2019;

Lei nº 12.682, de 9 de julho de 2012.

**7 Do Acesso Físico e Ambiental**

**7.1 Dos que podem ter acesso físico**

O público alvo de que trata o item 3 desta norma poderá ter o acesso físico mediante concordância tácita ou expressa dos gestores de negócio. Este deverá, sempre que solicitado, disponibilizar a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Federal da 2ª Região.

**7.2 Do acesso físico passível de concessão**

7.2.1 O acesso físico deverá se dar a partir da prévia autorização ao local de guarda, sucedida, preferencialmente, pela concomitante autenticação do usuário.

7.2.2 A autorização de acesso ao local de guarda deverá se dar por meio da concessão, pelo Gestor de Negócio, de permissão ao usuário ou grupo, para ingressar, circular, permanecer ou sair de locais, considerando as permissões de acesso, criticidade, ou prioridades de informação atribuídas.

7.2.3 Aplicam-se subsidiariamente as permissões e os perfis definidos para o acesso físico às instalações comuns (tais como portaria/recepção, hall de entrada, escadas, elevadores não privativos, corredores, banheiros, centrais de atendimento ao público externo, balcões/recepções, salas de audiências e sessões de julgamento, ouvidoria, bibliotecas, salas de leitura e cafeterias).

7.2.4 A permissão deverá ser individual e intransferível, sendo possíveis, no entanto, a herança de permissão e o regime de expressa substituição eventual.

7.2.5 Como preceito geral, deverá ser definido um perfil comum para a maioria das unidades e usuários, que exerce atividades sem peculiaridades técnicas relevantes, e determinados perfis especiais (tais como para administradores, técnicos, designers, editores, estagiários, empregados de "terceirizados", magistrados, advogados), com o mínimo privilégio, para as unidades e usuários que exercem atividades com peculiaridades técnicas relevantes.

7.2.6 A autenticação do usuário deverá se dar por meio de sua identificação, no local de guarda, perante o Gestor de Negócio, conforme seu anterior credenciamento, na portaria/recepção, pela unidade responsável pela infraestrutura ou segurança, em ACL - access control list (ou seja, lista de controle de acesso), baseada na credencial completa, composta:

- Pelo que se tem em termos de tecnologia (tal como crachá, distintivo, button, pin, broche, token, smartcard, selo, cartão de estacionamento etc.); ou
- Pelo que se é em termos de características biométricas (tal como mediante impressão digital, impressão palmar, caligrafia, formação da íris, voz, perfil genético etc.).

7.2.7 É aconselhável que o crachá seja o principal meio que compõe a credencial.

7.2.8 A credencial deverá ser individual e intransferível.

7.2.9 O crachá deverá:

- Ter especificações (tais como dimensões, cores, impressões etc.) que permitam fácil distinção visual do perfil do usuário;
- Ser colocado em local que permita fácil visualização e assim permanecer enquanto no interior das dependências da Justiça Federal da 2ª Região.

7.2.10 Todo local de guarda deverá, conforme os níveis de acesso, criticidade ou prioridade das informações nele guardadas:

- Ser dotado de infraestrutura inviolável ou de difícil violação, bem como portas e janelas passíveis de trancamento;
- Ter acesso restrito;
- Ser dotado de mobiliário inviolável ou de difícil violação e passível de trancamento, destinado ao armazenamento de suportes físicos de informações.

7.2.11 Todos os locais de guarda deverão se submeter a mapeamento e consequentes definições, pelas unidades responsáveis pela infraestrutura ou segurança, TI, documentação e segurança institucional, em conjunto com os respectivo Gestor de Negócio, dos respectivos níveis/perímetros de segurança, bem como dos PPS - perimeter protection systems (ou seja, sistemas de proteção de perímetro), baseados nos níveis de acesso, criticidade ou prioridade das informações nele guardadas.

7.2.12 Aplicam-se subsidiariamente o tombamento de todos os recursos materiais, as barreiras próprias da segurança física, as medidas especiais de tratamento de informações e a planilha da força de trabalho.

7.2.13 Sempre que possível:

- O credenciamento deverá compartilhar dados com o registro de incidentes de segurança da informação;
- O crachá e o cartão de estacionamento deverão ser dotados de fotografia digitalizada com alta resolução e colorida;
- O crachá e o cartão de estacionamento deverão ser dotados de transponder (transmissor) para RFID - radio-frequency identification (ou seja, identificação por radiofrequência) e, ao mesmo tempo, as dependências da Justiça Federal da 2ª Região deverão ser dotadas dos respectivos readers (leitores), tanto para ingresso quanto para circulação, permanência e saída;
- O crachá e o cartão de estacionamento deverão ter um prazo de validade, conforme a forma de vínculo ou as atividades exercidas;
- Todo local de guarda deverá ser dotado de porta com fechadura e chave eletromecânicas, bem como de mobiliário passível de trancamento da mesma espécie;
- A geração, entrega e alteração de segredo de cofre deverão se dar de modo a garantir a preservação do respectivo sigilo.

**7.3 Das finalidades do acesso físico**

7.3.1 O acesso físico deverá se dar em atividades imediatamente relacionadas ao serviço prestado na Justiça Federal da 2ª Região, na Escola da Magistratura Regional Federal da 2ª Região – EMARF, e no Centro Cultural da Justiça Federal – CCJF por lhe serem necessárias, e poderá se dar em atividades mediatamente relacionadas ao serviço nela prestado, por lhe serem úteis.

7.3.2 O acesso físico poderá se dar também em atividades não relacionadas ao serviço prestado na Justiça Federal da 2ª Região, na Escola da Magistratura Regional Federal da 2ª Região – EMARF e no Centro Cultural da Justiça Federal – CCJF desde que configurem práticas autorizadas.

**7.4 Das práticas de acesso físico**

7.4.1 O acesso físico deverá se dar de modo necessário ou útil ao serviço prestado na Justiça Federal da 2ª Região, Escola da Magistratura Regional Federal da 2ª Região – EMARF, e o Centro Cultural da Justiça Federal – CCJF.

7.4.2 O acesso físico não poderá se dar de modo ilícito, abusivo, anônimo ou com alto risco de impacto negativo, constatado pelo Gestor de Negócio, o que inclui, dentre outros similares:

- Interceptação, invasão, subtração, adulteração, prejuízo ou destruição de informações, mediante violação ou desativação de mecanismos de controle de segurança da informação;
- Exploração de vulnerabilidades;
- Obtenção de informações mediante fraude, ou de qualquer outra espécie de vantagem mediante fraude, num contexto de "engenharia social";

7.4.3 Enquanto o local de guarda estiver aberto, um servidor lotado na respectiva unidade, preferencialmente acompanhado de outro servidor, deverá:

- Estar presente e vigilante, ressalvada a possibilidade de permissão diversa pelo Gestor de Negócio, principalmente em situações de contingência, exceto se for alto o risco de impacto negativo;

- Supervisionar constantemente a utilização de dispositivos móveis de qualquer espécie destinados a reprodução de informações (tais como telefones, smartfones, gravadores, pen drives, cartões de memória, chips, câmeras, scanners e impressoras) ou aptos a eliminação de suportes físicos de informações, bem como o porte de acessórios para carregar objetos (tais como bolsas, sacos, sacolas e maletas) ou o uso de peças de vestuário aptas a carregarem objetos, conforme os níveis de acesso, criticidade ou prioridade das informações nele guardadas;
- Evitar situações aptas a prejuízo de sua atenção;
- Contar com o auxílio da unidade responsável pela infraestrutura ou segurança.

7.4.4 Se vier a estar inabitado, todo local de guarda deverá se submeter a trancamento, preferencialmente de modo eletrônico, ressalvada a possibilidade de permissão diversa pelo Gestor de Negócio, principalmente em situações de contingência, exceto se for alto o risco de impacto negativo.

7.4.5 Se o local de guarda não tiver se submetido a trancamento no fim do expediente, e não for a hipótese da ressalva descrita no item 7.4.4 desta Norma, ele deverá se submeter a lacre, pela unidade responsável pela infraestrutura ou segurança, no qual deverão constar o dia e hora de sua aposição.

**7.5 Do controle de acesso físico**

7.5.1 O controle de acesso físico, pela unidade responsável pela infraestrutura ou segurança:

- poderá ser preventivo, detectivo ou reativo, dando-se prévia, simultânea ou posteriormente, priorizando-se o primeiro;
- poderá ser ordinário ou extraordinário, gerando relatório periódico.

7.5.2 Poderão ser utilizados os seguintes mecanismos de controle:

- registros (tal como log) e manutenção preferencialmente durante o prazo para aplicar ou buscar a aplicação da penalidade para o tipo de infração mais grave;
- monitoramento de tráfego constante (tal como mediante a utilização de CFTV - circuito fechado de televisão);
- ronda;
- sensores, bem como de alarmes sonoros e visuais, com funcionamento constante;
- teste (tal como pentest) periódico;
- suspensão;
- invalidade;
- expulsão;
- inspeção periódica;

7.5.3 Sempre que tecnicamente possível, os mecanismos de controle, sempre atualizados, deverão ser ativados de modo automatizado (tal como mediante a utilização de detectores de metais, scanners de raios X, catracas/roletas e cancelas eletrônicas, detectores de abertura, presença e movimento, detectores de ondas eletromagnéticas), sem a possibilidade de desativação, ressalvada a possibilidade de revisão do resultado dessa automatização, a pedido ou de ofício, pelo Gestor de Negócio; e resguardada a plenitude da liberdade de locomoção.

7.5.4 Aplicam-se subsidiariamente os mecanismos de controle próprios da segurança física e de todos os recursos materiais, bem como o processo de gestão de riscos.

7.5.5 A danificação, extravio ou perda de qualquer chave, bem como a suspeita de perda do sigilo de segredo de cofre, deverão ser imediatamente reportados à unidade responsável pela infraestrutura ou segurança; e todos esses incidentes, bem como a execução de qualquer serviço de chaveiro (tal como de confecção, cópia de chave), a geração, entrega e alteração de segredo de cofre, e a abertura de qualquer fechadura sem chave ou segredo, deverão ser registrados por esta unidade.

7.5.6 Qualquer incidente que, envolvendo acesso físico, aparentemente tenha relevante risco de impacto negativo, deverá ser imediatamente reportado, por quem tomar conhecimento, ou mesmo de modo automatizado, ao respectivo Gestor de Negócio e à CLRI, para os devidos fins.

**7.6 Do Acesso Ambiental**

7.6.1 Para assegurar a proteção dos equipamentos, é necessário:

- Proteger os equipamentos fisicamente contra as ameaças à sua segurança e dos perigos ambientais.
- Planejar a localização e disposição dos equipamentos, de modo a reduzir o risco das ameaças e perigos do meio ambiente e as oportunidades de acesso não autorizado.
- Criar controles especiais para proteção contra perigos ou acesso não autorizado e para preservar os equipamentos de apoio, como o suprimento de corrente e a infraestrutura de cabeamento.
- Posicionar os equipamentos de processamento e armazenagem de informações que manuseiam dados sensíveis de modo a minimizar o risco de olhares indiscretos durante o uso.
- Isolar os itens que requerem proteção especial a fim de garantir o nível apropriado de proteção.
- Adotar controles para minimizar o risco de ameaças potenciais, incluindo furto, incêndio, fumaça, água (ou falha no abastecimento), poeira, vibração, efeitos químicos, interferência no suprimento de força e radiação eletromagnética
- Proibir comer, beber e fumar nas instalações de processamento de informações ou em sua proximidade.
- Monitorar as condições ambientais quanto a fatores que podem afetar negativamente a operação dos equipamentos de processamento de informações.
- Considerar o impacto de um acidente em instalações próximas, como por exemplo, um incêndio no prédio vizinho ou em outras empresas localizadas no mesmo prédio, vazamento de água do telhado, ou dos andares acima da EPE, ou uma explosão na rua.
- Proibir a identificação dos equipamentos de processamento de informações sensíveis nas listas de pessoal e listas telefônicas internas ou em locais acessíveis ao público.

7.6.2 Para assegurar a proteção dos documentos, é necessário:

- Proteger os documentos fisicamente contra as ameaças à sua segurança e dos perigos ambientais.
- Planejar a localização e disposição dos documentos, de modo a reduzir o risco das ameaças e perigos do meio ambiente e as oportunidades de acesso não autorizado.
- Criar controles especiais para proteção contra perigos ou acesso não autorizado.

- Isolar os documentos que requerem proteção especial a fim de garantir o nível apropriado de proteção.
- Adotar controles para minimizar o risco de ameaças potenciais, incluindo furto, incêndio, fumaça, água (ou falha no abastecimento), poeira, vibração e efeitos químicos.
- Proibir comer, beber e fumar nas instalações de guarda e processamento de documentos ou em sua proximidade.
- Monitorar as condições ambientais quanto a fatores que podem afetar negativamente conservação dos documentos.
- Considerar o impacto de um acidente em instalações próximas, como por exemplo, um incêndio no prédio vizinho ou em outras empresas localizadas no mesmo prédio, vazamento de água do telhado, ou dos andares acima da EPE, ou uma explosão na rua.
- Posicionar documentos críticos em local não acessível ao público.

7.6.3 Visando evitar exposição ou roubo de informações e de recursos de processamento da informação das salas e instalações, deve-se:

- Adotar procedimentos para garantir a política de mesa limpa e tela limpa.
- Posicionar equipamentos críticos em local não acessível ao público.
- Escolher salas discretas e que indiquem o mínimo possível a sua finalidade, sem sinais visíveis, dentro ou fora da sala, que identifiquem a presença de atividades de processamento de informações.
- Evitar a divulgação de detalhes da arquitetura da rede em acessos externos.
- Implantar sistemas apropriados de detecção de intrusos, instalados segundo padrões profissionais, e testados regularmente para cobrir todas as portas externas.
- Dispor, sempre que possível, alarme armado permanentemente nas áreas não ocupadas.
- Dispor equipamentos administrados pela organização fisicamente separados dos equipamentos administrados por terceiros.
- Armazenar de modo seguro e a uma distância adequada de uma área segura os materiais perigosos ou combustíveis.
- Posicionar a uma distância segura os equipamentos e mídia de backup, para que não sejam danificados em caso de um acidente no site principal da organização.

7.6.4 A fim de garantir o suprimento adequado de eletricidade que atenda às especificações dos fabricantes dos equipamentos, evitando-se quedas e oscilações de tensão frequentes e sobrecargas, deve-se:

- Manter plantas atualizadas da rede elétrica.
- Utilizar múltiplas fontes de alimentação para evitar que o suprimento dependa de uma única fonte, sempre que possível.
- Fornecer suprimento de energia à prova de interrupções (sistema no break) para os equipamentos dos CPDs e para os ativos críticos e/ou sensíveis.
- Providenciar um plano de contingência indicando as ações a serem tomadas em caso de falha do no break.
- Realizar testes periódicos dos equipamentos de suprimento de energia elétrica regulada, de acordo com as recomendações dos fabricantes, para assegurar que tenham a capacidade adequada.
- Localizar as chaves de força de emergência perto das saídas de emergência das salas de equipamentos.
- Ter iluminação de emergência para o caso de falta de energia elétrica.

- Verificar periodicamente se as instalações elétricas do prédio e as instalações destinadas aos equipamentos de energia estão em boas condições e não oferecem perigo.
- Garantir exclusividade das instalações elétricas no CPD.
- Manter um plano de manutenção para a rede elétrica.

7.6.5 Quanto às condições gerais de segurança relacionados com suprimento de água, deve-se:

- Manter plantas atualizadas da rede hidráulica.
- Retirar qualquer encanamento, exceto o necessário, do piso ou teto falso em áreas sob ou sobre as áreas seguras.
- Garantir escoamento de água e drenagem adequada para impedir inundação nas áreas seguras.

7.6.6 Quanto à segurança do cabeamento, deve-se:

- Dar proteção adequada às linhas de força e as linhas de telecomunicações.
- Proteger o cabeamento de rede contra interceptação não autorizada ou danos por meio da utilização de dutos, evitando trajetos que passem por áreas públicas.
- Sempre que possível, separar os cabos de força dos cabos de comunicações para evitar interferências.
- Sempre que possível, utilizar dutos blindados e salas ou caixas trancadas em pontos de inspeção e pontos terminais.
- Planejar o uso de rotas ou meios de transmissão alternativos.

7.6.7 Segurança no Descarte ou na Reutilização de Equipamentos e Materiais.

- No descarte ou na reutilização de equipamentos e materiais que contenham qualquer tipo de informação, deve-se atentar aos cuidados necessários conforme o tipo de equipamento e material e a informação neles contidos.
- Deve-se destruir fisicamente ou sobrescrever de maneira segura no lugar do uso da função delete, os sistemas de armazenagem que contenham informações sensíveis. Devem-se verificar todos os itens de equipamento que contenham mídia de armazenagem, como por exemplo, discos rígidos, para garantir que todos os dados sensíveis e softwares licenciados tenham sido retirados ou sobrescritos antes do descarte ou reutilização. Os dispositivos de armazenagem danificados devem ser avaliados quanto às informações neles contidos, para determinar a conveniência de serem consertados, descartados ou destruídos.
- Os materiais que contenham informações (CDs, papel etc.) devem ser destruídos de forma a impedir sua recomposição.

7.6.8 Quanto aos equipamentos de prevenção e combate a incêndios, produtos e locais críticos, deve-se:

- Manter a compatibilidade dos equipamentos de prevenção e combate a incêndios com o ambiente onde podem vir a ser necessários.
- Prover uma quantidade suficiente de equipamentos, mantendo-se uma margem para contingência.
- Distribuir os equipamentos em locais adequados e garantir o acesso livre aos mesmos.
- Conferir a validade das cargas dos equipamentos de combate a incêndio periodicamente.

- Instalar sensores e alarmes e mola para fechamento automático nas portas de incêndio.
- Instalar detectores de fumaça sob o piso falso, no teto e no sobre teto.
- Dispor os equipamentos distantes das linhas de transmissão de alta voltagem.
- Prover cestas de lixo de metal com tampa com objetivo de abafar princípios de incêndio.

7.6.9 A fim de zelar pela segurança da edificação, deve-se:

- Remover o lixo diariamente.
- Verificar periodicamente a necessidade de efetuar dedetização e desratização.
- Proibir a execução de trabalho que gerem poeira na área dos equipamentos, sem que sejam tomados os cuidados necessários para a execução dos mesmos.
- Manter trancados os quadros de conexões telefônicas e distribuição do cabeamento de rede e garantir que o acesso somente seja permitido ao pessoal autorizado.
- Manter e testar os detectores de fumaça de forma programada.
- Instalar sensores de temperatura e umidade do ar.
- Verificar a necessidade de suplementar os recursos condominiais com quadros de controle que detectem e localizem rapidamente fogo e fumaça.
- Utilizar placas do piso falso que sejam facilmente removíveis a fim de facilitar a verificação de fogo e fumaça.
- Manter marcações no piso para facilitar a localização dos detectores.
- Manter plantas de localização dos extintores e detectores.
- Manter sensoriamento de portas, janelas, dutos e supervisão predial.
- Ter uma sala central de controle de segurança bem localizada e com qualificação pessoal, mesmo que seja a do condomínio.
- Efetuar monitoramento do perímetro e áreas externas à empresa via CFTV.
- Prover a proteção adequada ou estabelecer perímetros de segurança para estações de trabalho e servidores não monitorados por um longo período de tempo (CPD), principalmente no que diz respeito ao acesso não autorizado.
- Manter a área do CPD em local não visível da rua.
- Manter as portas do CPD fechadas e com acesso controlado.
- Instalar alarmes para informar à vigilância ou a quem de direito, a violação de portas e acessos a áreas do CPD.
- Manter um serviço de vigilância de 24 horas, inclusive nos fins de semana e feriados.
- Verificar as saídas de emergência em relação à usabilidade periodicamente.
- Efetuar rodízio periódico entre os (as) recepcionistas.
- Manter uma rede de iluminação bem distribuída e de boa qualidade com iluminação de emergência.
- Fornecer manual ao corpo de vigilantes ou agentes prediais com procedimentos de emergência.
- Manter um sistema de claviculário na área de serviços gerais ou local adequado indicado por esta área.
- Manter um controle rigoroso das chaves das portas.
- Dispor de quadros de luz e iluminação em locais adequados.
- Manter o controle da temperatura nas imediações do perímetro.

7.6.10 A monitoração das instalações por CFTV visa à proteção dos ativos físicos e informacionais, devendo ser ao mesmo tempo compreensiva e privativa. Diante disso, o sistema de monitoração deve:

- Manter a privacidade das áreas de uso individual como a estação de trabalho.

- Cobrir todas as áreas de circulação, entradas e saídas.
- Cobrir todas as áreas de acesso restrito, tanto externa como internamente.
- Permitir a captura detalhada e resumida das imagens monitoradas.
- Possibilitar a retenção das imagens capturadas por um período não inferior a dois anos.
- Anunciar ostensivamente os locais sendo monitorados.

7.6.11 A visita às imagens capturadas deve guiar-se pelo seguinte:

- Ocorrer somente quando houver indícios de incidentes de segurança e para a verificação da eficácia do sistema.
- Ser feita sempre por mais de uma pessoa, concomitantemente.
- Ter um registro de quem acessou, quando e com que fim, bem como das imagens visitadas.

7.6.12 Quanto às questões de segurança relacionadas ao ar-condicionado, deve-se:

- Garantir a qualidade das instalações e manutenção dos equipamentos e em nível de ruído satisfatório.
- Eliminar a possibilidade de entrada de gases através dos dutos de ar-condicionado.
- Garantir que as chaves de emergência desliguem o sistema de ar-condicionado.
- Garantir que o sistema de climatização seja exclusivo e que não seja compartilhado com área e/ou tipo de equipamentos inadequados.
- Garantir que o dimensionamento do equipamento de ar-condicionado seja adequado.
- Garantir que as aberturas externas (troca de ar) proporcionem uma adequada renovação.
- Utilizar dampers corta-fogo e gases no interior dos dutos.
- Instalar os equipamentos de ar-condicionado em compartimentos fechados (com acesso somente ao pessoal autorizado).
- Proteger as tomadas de ar contra contaminação.
- Verificar a necessidade de existirem alarmes nos sistemas de ar-condicionado.
- Utilizar dutos do ar condicionado de material retardante da propagação de fogo.
- Proteger os instrumentos de comando do sistema de ar-condicionado prevenindo o acesso não autorizado.
- Manter plantas com especificações de toda a rede de ar-condicionado.

7.6.13 Quanto à manutenção e à retirada de bens e equipamentos, deve-se:

- Fornecer manutenção correta aos equipamentos para assegurar sua disponibilidade e integridade permanente, com a periodicidade e especificações recomendadas pelo fabricante.
- Somente realizar a manutenção e os reparos dos equipamentos com profissional autorizado, habilitado e treinado.
- Manter um registro de todos os defeitos suspeitos ou reais e de toda a manutenção preventiva e corretiva executada.

**8 Disposições Finais**

As unidades responsáveis deverão providenciar a implantação desta Norma bem como os pertinentes registros e divulgação das informações de que trata a Norma de Segurança de Acesso Físico e Ambiental.

**PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.**

- assinado eletronicamente -

**GUILHERME CALMON NOGUEIRA DA GAMA**
**Presidente**