PORTARIA Nº 1712/2023

Dispõe sobre as diretrizes de Gestão de Identidade e de Controle de Acessos no âmbito do Poder Judiciário do Estado do Ceará.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ (TJCE), no uso de suas atribuições legais e regimentais,

CONSIDERANDO os termos da Resolução do Conselho Nacional de Justiça (CNJ) n° 370/2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) e estabeleceu as diretrizes para sua governança, gestão e infraestrutura;

CONSIDERANDO os termos da Resolução do CNJ n° 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO os termos da Resolução do Órgão Especial do TJCE n° 15/2023, que atualiza a Política de Segurança da Informação no âmbito do Poder Judiciário do Estado do Ceará.;

CONSIDERANDO os termos da Portaria do CNJ n° 162, que aprovou protocolos e manuais criados pela Resolução CNJ n° 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ); e

CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação que visam a garantir a disponibilidade e a integridade de sistemas, aplicativos, dados e documentos digitais do Poder Judiciário do Estado do Ceará;

RESOLVE:

Art. 1º Definir as diretrizes de Gerenciamento de Identidade e de Controle de Acessos no âmbito do Poder Judiciário do Estado do Ceará, na forma do Anexo I desta portaria.

Art. 2º A Secretaria de Tecnologia da Informação (SETIN) deverá informar ao Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP), em até 180 (cento e oitenta) dias após publicação deste

normativo ato, o tempo necessário para adequar-se as normas nele descritas, no que diz respeito as suas competências.

Art. 3º Os casos não previstos deverão ser apreciados pelo Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP).

Art. 4° Esta Portaria revoga o Anexo V – Norma para controle de acesso (físico e lógico n° 05/NSI05/CGSI/TJCE, Portaria nº 1186/2018, do Tribunal de Justiça do Estado do Ceará.

Art. 5º Esta Portaria entra em vigor na data da sua publicação.

REGISTRE-SE, PUBLIQUE-SE E CUMPRA-SE.

GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, em Fortaleza, aos 25 de junho de 2023.

Desembargador Antônio Abelardo Benevides Moraes
Presidente do Tribunal de Justiça do Estado do Ceará

ANEXO I DA PORTARIA Nº 1712/2023

NORMA DE GERENCIAMENTO DE IDENTIDADE E CONTROLE DE ACESSO

Dos princípios gerais:

Art. 1° A presente norma tem como objetivo definir as diretrizes em relação ao gerenciamento de identidade e controle de acesso no âmbito do Poder Judiciário do Estado do Ceará.

Art. 2° Esta norma aplica-se a todos os usuários e usuárias de tecnologia da informação que possuem ou são responsáveis por uma conta, bem como qualquer forma de acesso com privilégios de "administrador" de rede, sistemas de informações, equipamentos locais, serviços e banco de dados no ambiente de Tecnologia da Informação do Poder Judiciário do Estado do Ceará.

Art. 3° Para efeitos deste ato normativo consideram-se:

I - **usuário(a**) de TIC: magistrados(as) e servidores(as) ocupantes de cargo efetivo ou em comissão, requisitados(as) e cedidos(as), desde que previamente autorizados(as), empregados(as)

de empresas prestadoras de serviços terceirizados, conveniados(as), consultores(as), estagiários(as), e outras pessoas que se encontrem a serviço da Justiça Estadual, utilizando em caráter temporário os recursos tecnológicos do Poder Judiciário do Estado do Ceará;

II - **conta de acesso:** código de acesso atribuído a cada usuário. A cada código de acesso é associada uma senha individual e intransferível, destinada a identificar o Usuário, permitindo-lhe o acesso aos recursos computacionais disponíveis; e

III - **administrador:** usuários que podem posuir contas que permitem acesso total e irrestrito a quaisquer recursos da rede, sistema ou serviço em que estão configuradas.

CAPÍTULO I

DO CONTROLE DE ACESSO FÍSICO

SEÇÃO I

Art. 4° controle de Acesso Físico:

I - os controles de acessos físicos visam restringir o acesso aos equipamentos, documentos e suprimentos do Poder Judiciário do Estado do Ceará e à proteção dos recursos computacionais, permitido apenas às pessoas autorizadas;

II - devem ser adotados controles que restrinjam a entrada e saída de visitantes, pessoal interno, equipamentos e mídias;

III - deve ser estabelecido perímetros de segurança e habilitado o acesso apenas de pessoal autorizado. No caso de sistemas críticos, convém que sejam criados ambientes reservados, de uso exclusivo, para abrigá-los;

IV - todo o pessoal envolvido em trabalhos de apoio, tais como a manutenção das instalações físicas, deve ser orientado e capacitado para manter a adoção de medidas de proteção ao acesso;

V - todas as pessoas devem portar algum tipo de identificação visível que informe se é um servidor ou não, bem como o nível de autorização de acesso;

VI - o ingresso de visitantes deve ser controlado de tal forma a impedir o acesso destes às áreas de armazenamento ou processamento de informações sensíveis, salvo acompanhados e com autorização do responsável;

VII - deverão ser criados procedimentos de acesso:

a) as dependências do Palácio da Justiça – TJCE, Corregedoria, Centro de Documentação e Informática – CDI e outras unidades do Poder Judiciário do Estado do Ceará que venham a ser

instaladas no Centro Administrativo Governador Virgílio Távora (Cambeba);

b) as dependências do Fórum Clóvis Beviláqua e demais unidades da Justiça Estadual na Comarca de Fortaleza;

c) as dependências do Fórum das Turmas Recursais, ESMEC e Creche Escola do Poder Judiciário e demais unidades da Capital; e

d) as dependências das unidades da Justiça Estadual nas Comarcas do interior do Estado do Ceará;

VIII - deverão ser criados procedimentos de acesso e segurança contra incêndios e outros desastres naturais:

a) nas dependências dos Datacenteres localizados no Centro de documentação e Informática – CDI, no Fórum Clóvis Beviláqua e outros a serem construídos;

b) aos setores que possuem equipamentos de rede, comunicação e dispositivos de TIC que estão fora dos Datacenteres e nas dependências dos prédios do Poder Judiciário do Estado do Ceará;

c) aos locais onde ficam instalados nobreaks e geradores que alimentam equipamentos e dispositivos de TIC nos ambientes dos Datacenteres e Racks de todas as Comarcas do Poder Judiciário do Estado do Ceará; e

d) aos locais onde ficam instalados equipamentos e dispositivos de telefonia.

SEÇÃO II

DOS EQUIPAMENTOS DE PROCESSAMENTO E ARMAZENAMENTO

Art. 5° Para evitar perdas, danos, furtos ou comprometimento de ativos e interrupção das operações da organização, o Tribunal deve observar as seguintes diretrizes:

I - adotar controles para minimizar o risco de ameaças físicas potenciais e ambientais, como furto, incêndio, explosivos, fumaça, água, poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;

II - verificar se os suprimentos de energia elétrica, telecomunicações, água, gás, esgoto, calefação/ventilação e sistema de ar-condicionado estejam em conformidade com as especificações do fabricante do equipamento e com os requisitos legais da localidade;

III- adotar controles para evitar a retirada de equipamentos do Tribunal sem prévia autorização da unidade competente, conforme regulamentação específica; e

IV- utilizar, sempre que possível, racks que disponham de fechaduras com chave ou mecanismo semelhante, garantindo que apenas a(s) equipe(s) responsáveis pelos ativos instalados nos racks tenham acesso físico a eles.

SEÇÃO III

DA SEGURANÇA DO CABEAMENTO

Art. 6° O cabeamento de energia elétrica e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos, conforme as seguintes diretrizes:

I - as linhas de energia elétrica e de telecomunicações que entram nas instalações de processamento da informação devem ser subterrâneas ou ficar abaixo do piso, sempre que possível, e devem atender aos requisitos mínimos de proteção; e

II - os cabos de energia elétrica devem ser segregados dos cabos de comunicação, para evitar interferências.

SEÇÃO IV

DA MANUTENÇÃO EXTERNA DOS EQUIPAMENTOS

Art. 7° A manutenção dos equipamentos de processamento de informações deve seguir as seguintes diretrizes:

I - ser realizada somente por pessoal de manutenção identificado e autorizado;

II - manter registro de todas as falhas, constatadas ou suspeitas, e de todas as operações de manutenção preventiva e corretiva realizadas;

III - eliminar as informações sensíveis do equipamento, quando possível, ou tratar de forma alternativa os riscos de sua exposição;

IV - inspecionar o equipamento, após a manutenção, para garantir que não foi alterado indevidamente e que está em perfeito funcionamento.

SEÇÃO V

DA REUTILIZAÇÃO OU DESCARTE SEGURO DOS EQUIPAMENTOS OU DOS EQUIPAMENTOS EM PROVA DE CONCEITO

Art. 8° Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização ou descarte, para assegurar que dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.

Parágrafo único. As mídias que contenham informações com acesso restrito de propriedade intelectual devem ser apagadas fisicamente. Da mesma forma, as informações devem ser destruídas, apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis.

CAPÍTULO II

DO CONTROLE DE ACESO LÓGICO

SEÇÃO I

Art. 9° Os controles de acesso lógico são um conjunto de procedimentos, recursos e meios utilizados com a finalidade de prevenir e/ou obstruir ações de qualquer natureza que possam comprometer recursos computacionais, redes corporativas, aplicações e sistemas de informação;

Art. 10. Os locais que abrigam meios de comunicação devem ser protegidos para evitar a interceptação e/ou interferência de dados;

Art. 11. Os computadores, equipamentos e dispositivos de TIC e sistemas do Poder Judiciário do Estado do Ceará devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados.

Art. 12. O acesso lógico aos recursos da Rede Local e aos sistemas deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela Secretaria de Tecnologia da Informação, baseado nas responsabilidades e tarefas de cada usuário, observando os itens:

I - terão direito a acesso lógico aos recursos da Rede Local e aos sistemas os usuários de recursos de tecnologia da informação.

II - para fins deste normativo, consideram-se usuários de recursos de tecnologia da informação os usuários definidos no Inciso I, Art. 3° deste normativo.

III - o acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, ou outra tecnologia disponibilizada pela Secretaria de Tecnologia da Informação, após as devidas autorizações.

IV - deve ser utilizado a Autenticação Multifator, Multi Factor Authentication (MFA) para a autenticação de acesso remoto.

V - o acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA.

VI - a concessão e a revogação de acesso serão implementadas por meio de um processo formal, preferencialmente automatizado, com estabelecimento de responsáveis pela

solicitação, administração, concessão, bloqueio e revogação.

§ 1° Compete aos proprietários de todos os tipos de ativos estabelecer regras de concessão, bloqueio e revogação de acesso aos ativos para os usuários, levando em conta as políticas, princípios e normas de controle de acesso aplicáveis.

§ 2° Os acessos deverão ser retirados imediatamente após a revogação dos direitos ou o encerramento das atividades, contratos ou acordos, ou ajustados após qualquer mudança de atribuições.

§ 3° As contas deverão ser desabilitadas, em vez de excluídas, para preservação de trilhas de auditoria.

§ 4° A criação de nomes de usuário e de contas de e-mail seguirá critério padronizado.

Art. 13. A Coordenadoria de Segurança da Informação, deve estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviço. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

I - unidade proprietária.

II - data de criação/última autorização de renovação de acesso;

III - a Coordenadoria de Segurança da Informação, deve e é responsável por validar todas as contas ativas a cada 45 (quarenta e cinco) dias.

Art. 14. A Coordenadoria de Segurança da Informação deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

Art. 15. A Coordenadoria de Segurança da Informação deve estabelecer e manter um inventário dos sistemas de autenticação e autorização, tal inventário deve ser revisado periodicamente.

Art. 16. A Coordenadoria de Segurança da Informação deve centralizar o controle de acesso para todos os ativos de informação do Poder Judiciário do Estado do Ceará (PJCE) por meio de um serviço de diretório ou provedor de SSO.

Art. 17. A Coordenadoria de Segurança da Informação deve definir e manter o controle de acesso dos usuários baseado em funções.

I- o modelo de controle de acesso será, preferencialmente fundamentado no controle de acesso baseado em papéis (RBAC), em que as credenciais recebam os privilégios de acesso conforme os papéis e as responsabilidades executadas pelos usuários;

II - deve ser elaborada a documentação dos direitos dos acessos para cada função dentro do PJCE.

III - a Coordenadoria de Segurança da Informação deverá realizar análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

SEÇÃO II

DA CONTA DE ACESSO LÓGICO, SENHA , ACESSO À INTRANET E AOS SISTEMAS DE TECNLOGIA DA INFORMAÇÃO

Art. 18. Para utilização das estações de trabalho do PJCE, será obrigatório o uso de uma conta de rede com única identificação (login) e de senha de acesso, fornecidos pela Secretaria de Tecnologia da Informação, mediante solicitação formal pelo titular da unidade do requisitante.

I. A solicitação deve ocorrer por chamado Via CatiNet ou por processo administrativo.

II. Os privilégios de acesso dos usuários à Rede Local devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

III. Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para a Coordenadoria de Segurança da Informação que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 19. O login e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela Coordenadoria de Segurança da Informação quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 20. O padrão adotado para o formato da conta de acesso do usuário é o estabelecido no documento critérios de padronização de nome de usuário e conta de e-mail, disponibilizado na base de conhecimento de TI.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, a Coordenadoria de Segurança da Informação realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 21. Acesso a recursos da Intranet:

I - o Poder Judiciário do Estado do Ceará utiliza o Active Directory (AD) para controlar o acesso dos usuários/administradores a rede e seus recursos;

II - para a concessão ou revogação dos acessos à rede para os magistrados, servidores

ocupantes de cargo efetivo ou em comissão, terceirizados contratados pela Secretaria de Gestão de Pessoas – SGP, requisitados, cedidos, estagiários, deverão ser considerados os requisitos abaixo:

a) estar em pleno exercício de suas atividades e cadastrados no Sistema ADMRH Gestão de Recursos Humanos ou Cadastrados no Sistema de Cadastro Geral de Vínculos, ou autorizado pelo CGSICCPDP;

b) a solicitação de acesso a rede do TJCE e criação da conta de e-mail institucional deverá ser realizada pelo gestor da unidade de lotação; e

c) cessado o motivo da concessão, o gestor da unidade de origem, ou seu substituto, deverá requerer à Secretaria de Tecnologia da Informação (Setin), a imediata desabilitação do usuário do perfil;

III - para a concessão ou revogação dos acessos à rede para os servidores/funcionários de Órgãos Públicos ou Instituições Particulares conveniadas deverão ser considerados os requisitos abaixo:

a) existência de cláusulas nos convênios que preveem concessão de acesso à rede, bem como a necessidade de acessar os serviços computacionais do Poder Judiciário do Estado do Ceará;

b) estar em pleno exercício de suas atividades e cadastrados no Sistema ADMRH Gestão de Recursos Humanos ou Cadastrados no Sistema de Cadastro Geral de Vínculos, ou autorizado pelo CGSICCPDP;

c) a solicitação de acesso a rede do TJCE e criação da conta de e-mail institucional deverá ser realizada pelo gestor da unidade de lotação e autorizada pelo responsável pelo convênio por parte do TJCE; e

d) cessado o motivo da concessão, o responsável pelo convênio por parte do TJCE, deverá requerer a imediata revogação do perfil junto à Secretaria de Tecnologia da Informação (Setin);

IV) para a concessão ou revogação dos acessos à rede do TJCE para funcionários de empresas contratadas pelo TJCE para prestação de serviços, deverão ser considerados os requisitos abaixo:

a) existência de cláusulas em contratos/acordos que preveem o acesso à rede, bem como a necessidade de acesso aos serviços computacionais do Poder Judiciário do Estado do Ceará, devendo ainda constar Termo de Ciência do Termo de Compromisso ou Termo assinado para contratos de Tecnologia da Informação ou de Confidencialidade para outras contratações.

b) a solicitação de acesso a rede do TJCE a funcionários lotados fisicamente nas dependências do Poder Judiciário do Estado do Ceará ou à serviço de forma remota deverá ser

realizada pela equipe gestora do contrato.

c) estar em pleno exercício de suas atividades, contrato com o TJCE vigente e possuir vínculo com a empresa contratada, bem como cadastrado no Sistema de Cadastro Geral de Vínculos, ou autorizado pelo CGSICCPDP;

d) cessado o motivo da concessão, a equipe gestora do contrato deverá requerer a imediata revogação do perfil à Secretaria de Tecnologia da Informação (Setin);

V - não serão concedidos acessos à rede, a usuários genéricos;

VI - o acesso como administrador da máquina local só será concedido nos seguintes casos:

a) para servidores do Poder Judiciário do Estado do Ceará da área de Tecnologia da Informação, quando solicitado pelos gestores de suas respetivas áreas, com as devidas justificativas, e autorizado pela Coordenadoria de Segurança da Informação;

b) para usuários de empresas prestadoras de serviços de TI ou terceirizados da área de TI, quando solicitado pelos fiscais do contrato ou o gestor do terceirizado da área de TI, com as devidas justificativas, e autorizado pela Coordenadoria de Segurança da Informação; e

c) para os demais casos, deverá ser solicitado à Coordenadoria de Segurança da Informação, que após análise, submeterá ao Coordenador do Grupo de Apoio Técnico ao CGSICCPDP;

VII - terá direito ao uso da Rede Privada Virtual – RPV, os usuários(a) de TIC a serviço do Poder Judiciário do Estado do Ceará, desde que atendam os seguintes requisitos:

a) com vínculo permanente com o PJCE e verificado nos sistemas ADMRH ou SCGV;
b) Na ausência de vínculo permanente, a solicitação deverá ser encaminhada à Coordenadoria de Segurança da Informação, para análise.

VIII - Durante a implantação de sistemas em ambientes de treinamento ou homologação, a equipe de fiscalização e gestão de contratos da área de TI, poderá solicitar ao Coordenador de Segurança da Informação acesso via VPN para funcionários de empresas que prestam serviços ao TJCE, desde que solicitado pelo preposto do contrato e devidamente justificado.

IX - não serão concedidos acessos à rede e aos seus recursos, a usuários que não possuam vínculos formais com Poder Judiciário do Estado do Ceará, exceto quando autorizados pela Coordenadoria de Segurança da Informação e com o de acordo da Gerencia de Infraestrutura de TI.

Art. 22. Da concessão de Acesso aos Sistemas Judiciais e Administrativos:

I - para a concessão ou revogação dos acessos aos Sistemas Judiciais e Administrativos

para os magistrados, servidores ocupantes de cargo efetivo ou em comissão, terceirizados contratados pela Secretaria de Gestão de Pessoas – SGP, requisitados, cedidos, estagiários, deverão ser considerados os requisitos abaixo:

a) estar em pleno exercício de suas atividades, possuir acesso a rede do TJCE estar ativo no Sistema ADMRH Gestão de Recursos Humanos ou ativo no Sistema de Cadastro Geral de Vínculos, ou autorizado pelo Gestor ou Gestora do Sistema ou CGSICCPDP;
b) a solicitação de acesso deverá ser realizada pelo gestor da unidade de lotação de acordo com os procedimentos estabelecidos pelo Gestor ou Gestora do Sistema; e
c) cessado o motivo da concessão, o gestor da unidade de origem, ou seu substituto, deverá requerer à Secretaria de Tecnologia da Informação (Setin), a imediata desassociação do usuário do perfil.

II - para a concessão ou revogação dos acessos dos servidores/funcionários de Órgãos Públicos ou Instituições Particulares conveniados aos Sistemas Judiciais e Administrativos, deverão ser considerados os requisitos abaixo:

A) existência de cláusulas nos convênios que preveem concessão de acesso à rede, bem como a necessidade de acessar os sistemas computacionais do Poder Judiciário do Estado do Ceará;
B) a solicitação de acesso deverá ser realizada pelo gestor da unidade de lotação mediante comprovação de que o usuário possui acesso a rede do TJCE e autorizada pelo responsável pelo convênio por parte do TJCE de acordo com os procedimentos estabelecidos pelo Gestor ou Gestora do Sistema;
C) cessado o motivo da concessão, o responsável pelo convênio por parte do TJCE, deverá requerer a imediata revogação do perfil junto à Secretaria de Tecnologia da Informação (Setin).

III - para a concessão ou revogação dos acessos de funcionários de empresas contratadas pelo TJCE para prestação de serviços, aos Sistemas Judiciais e Administrativos, deverão ser considerados os requisitos abaixo:

a) existência de cláusulas em contratos/acordos que preveem o acesso aos Sistemas Judiciais e Administrativos, bem como a necessidade de acessar os serviços computacionais do Poder Judiciário do Estado do Ceará, devendo ainda constar Termo de Ciência assinado para contratos de Tecnologia da Informação;
b) a solicitação de acesso aos Sistemas Judiciais e Administrativos do TJCE a funcionários lotados fisicamente nas dependências do Poder Judiciário do Estado do Ceará deverá ser realizada pela equipe gestora do contrato mediante

comprovação de que o usuário possui acesso a rede do TJCE e de acordo com os procedimentos estabelecidos pelo Gestor ou Gestora do Sistema; e

c) cessado o motivo da concessão, a equipe gestora do contrato deverá requerer a imediata revogação do perfil à Secretaria de Tecnologia da Informação (Setin).

IV - não serão concedidos acessos aos Sistemas Judiciais e Administrativos e aos seus recursos:

a) a usuários que não possuam acesso à Rede do TJCE e não possuam vínculos formais com Poder Judiciário do Estado do Ceará; e

b) e a usuários genéricos.

Art. 23. Da definição dos perfis para acesso aos Sistemas Judiciais e Administrativos:

I - apenas usuários autorizados terão acesso aos recursos de sistemas com perfis bem definidos e acesso apenas aos recursos realmente necessários para a execução de suas tarefas;

II - Os usuários devem ser impedidos de executar operações incompatíveis com as atribuídas a seu perfil.

III - os usuários dos Sistemas Judiciais e Administrativos deverão ser identificados e autenticados (logon).

IV - os gestores dos sistemas em conjunto com o analista da área de Tecnologia da Informação deverão definir os perfis de acesso aos Sistemas Judiciais e Administrativos, estabelecendo as atribuições de cada perfil.

V - os gestores de Sistemas Judiciais e Administrativos estabelecerão os procedimentos para a concessão e revogação dos acessos, de forma a complementar esta norma, contemplando: os perfis e a forma de solicitar e revogar os acessos;

VI - os gestores de Sistemas Judiciais e Administrativos concederão e revogarão os acessos aos usuários do sistema, de acordo com os perfis estabelecidos, diretamente no sistema, quando houver viabilidade técnica, ou através de solicitação à Central de Atendimento em Tecnologia da Informação (CATI);

VII - todos os perfis, suas atribuições, os procedimentos para concessão e revogação dos acessos definidos pelos gestores de Sistemas Judiciais e Administrativos, deverão ser encaminhados à Central de Atendimento de Tecnologia da Informação – CATI; e

VIII - quando não houver definição de perfis, suas atribuições, procedimentos para concessão e revogação dos acessos aos Sistemas Judiciais e Administrativos, o usuário deverá ser orientado a solicitar o acesso ao sistema através de processo administrativo para o gestor ou gestora do referido sistema.

SEÇÃO III

DO BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 24. A conta de acesso será bloqueada nos seguintes casos:

I - após 5 (cinco) tentativas consecutivas de acesso errado;

II - solicitação do superior imediato do usuário com a devida justificativa;

III - quando da suspeita de mau uso dos serviços disponibilizados pelo Poder Judiciário do Estado do Ceará ou descumprimento da Política de Segurança da Informação – PSI e normas correlatas em vigência.

IV - após 45 (quarenta e cinco) dias consecutivos sem movimentação pelo usuário.

Art. 25. O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário a Coordenadoria de Segurança da Informação.

Art. 26. Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou do Setor responsável pela Gestão de Pessoas.

Art. 27. A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

Art. 28. A Gerência de Infraestrutura de TI deve configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido. Tal prazo pode ser específico para cada tipo de ativo.

Art. 29. A Gerência de Infraestrutura de TI deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

SEÇÃO IV

DA MOVIMENTAÇÃO INTERNA

Art. 30. Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados.

I - o novo superior imediato ou o Setor responsável pela Gestão de Pessoas deve realizar a solicitação de novos acessos de acordo com novo setor / função do usuário.

II - os direitos de acesso antigos devem ser imediatamente cancelados/desabilitados conforme solicitação do antigo superior imediato ou do Setor responsável pela Gestão de Pessoas.

CAPÍTULO III

SEÇÃO I

DA CONTA DE ACESSO BIOMÉTRICO

Art. 31. A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

Parágrafo único. O Poder Judiciário do Estado do Ceará tratará os respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO IV

SEÇÃO I

DO CONTROLE DE ACESSO AO CÓDIGO-FONTE DE PROGRAMAS

Art. 32. O código-fonte e itens associados (esquemas, especificações, planos de validação, etc) dos sistemas de informação desenvolvidos pelo Tribunal somente serão acessíveis pelos usuários que tenham como atribuição funcional seu desenvolvimento, manutenção ou outra atividade para a qual o acesso seja imprescindível.

§ 1º As bibliotecas de código-fonte e itens associados devem ser armazenadas em ferramentas apropriadas para este fim, em ambientes segregados dos sistemas operacionais onde os respectivos sistemas de informação sejam executados.

§ 2º Os eventos de acesso às bibliotecas de código-fonte e itens associados devem ser registrados, permitindo sua auditoria.

§ 3º Os códigos-fonte que sejam publicados para entidades externas devem contar com controles adicionais que garantam sua integridade.

CAPITULO V

SEÇÃO I

DOS ACESSOS PRIVILEGIADOS DOS ADMINISTRADORES

Art. 33. A utilização de identificação (login) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

I - somente os técnicos/analistas das Gerências de Tecnologia da Informação, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede, quando autorizados por suas gerências e pela Coordenadoria de Segurança da Informação.

II - na necessidade de utilização de login com privilégio de administrador do equipamento local, os requisitos devem ser de acordo com o inciso VI, Art. 21. Deste normativo, cuja solicitação poderá ser negada pela área de Segurança da Informação os casos em que entender desnecessária a utilização.

III - se concedida a permissão ao usuário como administrador local na estação de trabalho/notebook, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal da Gerência de Infraestrutura de TI].

IV - caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

V - a identificação (login) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

VI - salvo para atividades específicas da área responsável pela gestão da tecnologia da informação, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

VII - o acesso privilegiado deve ser concedido ao usuário por meio de credenciais de acesso exclusivas para este fim, distintas das credenciais de acesso concedidas a tal usuário para a

realização de suas atividades normais de negócio.

VIII - o procedimento de concessão de acesso privilegiado deve manter arquivo de registro contendo informações sobre este pedido para posterior auditoria.

IX- o Gestor do ativo de informação deve definir prazos de expiração para as credenciais de acesso privilegiado, após os quais deve ser reavaliado o atendimento aos critérios para a atribuição de acesso privilegiado ao detentor das credenciais expiradas.

X - a solicitação de acesso privilegiado para qualquer unidade que não seja gestora do ativo deverá ser encaminhada através de processo administrativo ao Coordenador d CGSICCPDP, para análise e autorização.

XI - as competências dos usuários com acesso privilegiado aos sistemas e ativos de informação deverão ser avaliadas em intervalos não superiores a um mês, para que estejam alinhadas às atividades e obedecendo as regras de segregação de funções.

XII - o acesso privilegiado aos sistemas e ativos de informação através do uso de ID de usuário administrador genérico deve ser evitado, se o sistema assim permitir e, quando não houver

esta possibilidade, deve ser concedido mediante procedimentos de troca periódica de senha e auditoria dos acessos, criados pelo gestor do ativo.

A) após a saída ou mudança de lotação de usuário com conhecimento de senha de usuário administrador genérico, esta deve ser modificada.

B) a conta de administrador genérico deve ser renomeada e ter sua função apagada, para que não possa ser facilmente identificada.

C) a conta de administrador genérico não deve ser usada para acesso à Internet, iniciar serviços de rede e acessar arquivos externos.

D) a criação de conta de administrador genérico sempre deverá ser aprovada pelo Coordenador de Segurança da Informação e sempre deverá ter um servidor responsável pelo uso de tal conta.

XIII - excepcionalmente, poderão ser concedidas identificações (login) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação do Coordenador de Segurança da Informação por meio da Coordenadoria de Segurança da Informação.

XIV - a Coordenadoria de Segurança da Informação deve implementar o MFA para todas as contas de administrador.

XV - a Coordenadoria de Segurança da Informação deve restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador não consiga realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário.

CAPÍTULO V

SEÇÃO I

DAS RESPONSABILIDADES

Art. 34. É de responsabilidade do gestor imediato do usuário comunicar formalmente ao Setor responsável pela Gestão de Pessoas e à Coordenadoria de Segurança da Informação o desligamento ou saída do usuário do Poder Judiciário do Estado do Ceará para que as permissões de acesso à Rede Local e demais sistemas/serviços sejam canceladas/desabilitadas, mantendo-se as trilhas de auditoria.

Art. 35. Caberá ao Setor responsável pela Gestão de Pessoas do Poder Judiciário do Estado do Ceará, a comunicação imediata a Coordenadoria de Segurança da Informação sobre desligamentos, férias e licenças de magistrados, servidores e estagiários e usuários de TIC sob sua

gestão, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

Art. 36. É responsabilidade do Setor responsável pela gestão de mão-de-obra terceirizada e pelos fiscais/gestores de contrato/convênio/acordos do Poder Judiciário do Estao do Ceará a comunicação imediata a Coordenadoria de Segurança da Informação da Informação sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

I - os serviços serão filtrados por programas de antivírus, anti-phishing e anti-spam e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.

II - nenhum técnico da Secretaria de Tecnologia da Informação terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores do Poder Judiciário do Estado do Ceará, salvo se autorizado, por autoridade competente, para resolução de incidentes que envolvam segurança das informações.

Art. 37. É de responsabilidade da Gerência de Infraestrutura de TI o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do Poder Judiciário do Estado do Ceará.

Art. 38. É de responsabilidade da Assistência Militar:

I - criar procedimentos em relação aos acessos físicos as unidades, áreas críticas, áreas de armazenamento e processamento de informações do Poder Judiciário do Estado do Ceará; e

II - comunicar imediatamente a autoridade superior o descumprimento desta

norma. Art. 39. É de responsabilidade dos gestores de Sistemas:

II - definir os perfis de acesso aos sistemas, estabelecendo as atribuições de cada perfil, bem como conceder e revogar os acessos concedidos aos usuários do sistema de acordo com esses perfis, diretamente no sistema ou através de solicitação à Central de Atendimento em Tecnologia da Informação – CATI.

III - estabelecer procedimentos para a concessão de acesso, contemplando: os perfis de acesso ao sistema, quem poderá ter acesso ao sistema e qual a forma de solicitar o acesso.

IV - autorizar, conceder e revogar acesso a rede e aos sistemas sob sua gestão, aos usuários de outras instituições quando solicitados pelo gestor do Convênio, observando o item 4.2.7.4 desta norma.

V - definir os perfis adequados de acesso para auditorias e inspeções internas e externas.

Art. 40. O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade do Poder Judiciário do Estado do Ceará.

I - o usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

II - a utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

III - o usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 41. O usuário deve informar a Gerência de Infraestrutura de TI qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 42. É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para o PJCE, a saber:

I - não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II - evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III - interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV - não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V - não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI - utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas; E

VII - não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis.

CAPÍTULO VI

DISPOSIÇÕES GERAIS

Art. 43. Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários ao [Setor responsável pela Tecnologia da Informação].

Art. 44. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Gerência de Infraestrutura de TI fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização, observando os itens:

I - nos casos em que o autor da quebra de segurança for um usuário, a Gerência de Infraestrutura de TI comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis;

II - ações que violem a Política de Segurança da Informação (PSI) ou a Política Gral de Proteção de Dados Pessoais (PGPDP) ou que quebrem os controles de Segurança da Informação serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente;

III - processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela PSI ou a PGPDP; e

IV - resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo CGSICCPDP do Poder Judiciário do Estado do Ceará.