Estado do Ceará
Poder Judiciário
Tribunal de Justiça
Comitê Gestor de Segurança da Informação
Anexo V

PJSETIN2015004 – Implantação do Programa de Segurança Corporativa da Informação no âmbito do Poder Judiciário do Estado do Ceará

05/NSI05/CGSI/TJCE – **Norma para controle de acesso (físico e lógico)**

Sumário

1 Objetivo.....3
2 Abrangência.....3
3 Termos e Definições.....3
4 Diretrizes.....4
5 Competências e Responsabilidades.....11
6 Prazos e dos Controles.....12
7 Penalidades.....13
8 Vigência.....13

1 **Objetivo**

1.1 Definir as diretrizes relacionadas ao controle de acesso lógico e físico no âmbito do Poder Judiciário do Estado do Ceará.

2 **Abrangência**

2.1 Esta norma se aplica no âmbito do Poder Judiciário do Estado do Ceará.

2.2 A partir da publicação desta norma todos os sistemas computacionais solicitados (comprados ou desenvolvidos internamente ou por terceiros) deverão atender os requisitos estabelecidos neste documento.

2.3 A partir da publicação desta norma todos os sistemas computacionais desenvolvidos por outros órgãos e doados ao Tribunal de Justiça do Estado do Ceará – TJCE, ou adquiridos através de licenças do tipo GNU General Public License (GPL) não estarão obrigados ao cumprimento dos requisitos estabelecidos neste documento.

2.4 Os sistemas computacionais solicitados (comprados, desenvolvidos por outros órgãos e doados ao TJCE ou adquiridos através de licenças do tipo GNU General Public License (GPL), ou desenvolvidos internamente ou por terceiros), antes da publicação desta norma, não estarão obrigados ao cumprimento dos requisitos estabelecidos neste documento.

2.5 Poderá o Gestor de Sistema solicitar à Setin estudo de viabilidade técnica para verificar a possibilidade de aplicar os requisitos deste documento aos sistemas solicitados anterior a publicação desta norma.

3 **Termos e Definições**

3.1 Usuário: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, conveniados, consultores, estagiários, e outras pessoas que se encontrem a serviço do Poder Judiciário do Estado do Ceará, utilizando em caráter temporário os recursos tecnológicos do Poder Judiciário do Estado do Ceará;

3.2 Gestor de sistema: responsável por coordenar os trabalhos relativos ao sistema de informação que trata da sua área de negócio e/ou conhecimento, bem como definir os requisitos funcionais que o sistema deve atender;

3.3 Administrador: usuários que possuem contas que permitem acesso total e

irrestrito a quaisquer recursos do sistema em que estão configuradas.

3.4 Órgão Público: qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

3.5 Software: é um conjunto de programas de computador, que realiza procedimentos, dotado de regras, documentos e dados associados que fazem parte das operações do Sistema de Computação

3.6 Áreas críticas de Tecnologia da Informação e Comunicação- TIC: são áreas de armazenamento e processamento de informações relativas aos sistemas corporativos do Poder Judiciário do Estado do Ceará, ambientes que possuem equipamentos de rede e telefonia, bem como, equipamentos (no breaks, geradores etc) que dão sustentação às áreas de armazenamento e processamento de informações relativas aos sistemas corporativos.

4 **Diretrizes**

4.1 **Controle de Acesso Físico**

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.

4.1.1 Devem ser adotados controles que restrinjam a entrada e saída de visitantes, pessoal interno, equipamentos e mídias.

4.1.2 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.

4.1.3 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.

4.1.4 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.

4.1.5 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.

4.1.5.1 Deverá ser adotado medidas para coleta e armazenamento deste registro deste ingresso.

4.1.6 Deverão ser criados procedimentos de acesso:

4.1.6.1 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);

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

4.1.6.3 as dependências do Fórum das Turmas Recursais, ESMEC e Creche Escola do Poder Judiciário; e

4.1.6.4 as dependências das unidades da Justiça Estadual nas Comarcas do interior do Estado do Ceará.

4.1.7 Deverão ser criados procedimentos contra incêndios e outros desastres naturais:

4.1.7.1 Para dependências dos Data Centers localizados no Centro de documentação e Informática – CDI, no Fórum Clóvis Beviláqua e outros a serem construídos;

4.1.7.2 Para setores que possuem equipamentos de rede, comunicação e dispositivos de Infraestrutura de TIC que estão fora dos Data Centers e nas dependências dos prédios do Poder Judiciário do Estado do Ceará;

4.1.7.3 Para os locais onde ficam instalados no breaks e geradores que alimentam equipamentos e dispositivos de Infraestrutura de TIC nos ambientes dos Data centers e Racks de todas as Comarcas do Poder Judiciário do Estado do Ceará; e

4.1.7.4 Para os locais onde ficam instalados equipamentos e dispositivos de telefonia.

4.1.8 Deverão ser criados procedimentos de acesso:

4.1.8.1 Para as dependências dos Data Centers localizados no Centro de documentação e Informática – CDI, no Fórum Clóvis Beviláqua e outros a serem construídos;

4.1.8.2 Para os setores que possuem equipamentos de rede, comunicação e dispositivos de Infraestrutura de TIC que estão fora dos Data Centers e nas dependências dos prédios do Poder Judiciário do Estado do Ceará;

4.1.8.3 Para os locais onde ficam instalados no breaks e geradores que alimentam equipamentos e dispositivos de Infraestrutura de TIC nos ambientes dos Data centers e Racks de todas as Comarcas do Poder Judiciário do Estado do Ceará; e

4.1.8.4 Para os locais onde ficam instalados equipamentos e dispositivos de telefonia.

4.2 **Controle de Acesso Lógico**

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.

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

4.2.2 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.

4.2.3 Os sistemas devem ser avaliados pela área de Sistemas com relação aos requisitos de segurança definidos no Plano de Desenvolvimento de Software – PDS, e em outros normativos em vigor, antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas.

4.2.4 **Acesso a recursos da Intranet**

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

4.2.4.2 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:

4.2.4.2.1 estar em pleno exercício de suas atividades e cadastrados no Sistema de Gerenciamento de Recursos Humanos (GRH);

4.2.4.2.2 a solicitação de acesso a rede do TJCE e criação da conta de e-mail institucional poderá ser realizada tanto pelo usuário titular quanto pelo seu gestor imediato através de registro de chamado pela CATI; e

4.2.4.2.3 cessado o motivo da concessão, o gestor da unidade atual de lotação, ou seu substituto, deverá requerer à Secretaria de Tecnologia da Informação (Setin), a desativação do acesso à rede e conta de e-mail.

4.2.4.3 Para a concessão ou revogação dos acessos dos servidores/funcionários de Órgãos Públicos ou Instituições Particulares conveniados, à rede, deverão ser considerados os requisitos abaixo:

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

4.2.4.3.2 estar em pleno exercício de suas atividades e cadastrados no Sistema de Gerenciamento de Recursos Humanos (GRH).

4.2.4.3.3 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.

4.2.4.3.4 cessado o motivo da concessão, o gestor da unidade, deverá requerer a imediata desativação dos acessos de rede e conta de e-mail junto à Secretaria de Tecnologia da Informação (Setin).

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

4.2.4.4.1 existência de cláusulas em contratos/acordos que prevejam o acesso aos recursos de TI necessários à execução do contrato, devendo ainda constar Termo de Ciência assinado para contratos de Tecnologia da Informação.

4.2.4.4.2 a solicitação de acesso a rede do TJCE a funcionários lotados fisicamente nas dependências do Poder Judiciário do Estado do Ceará deverá ser autorizada pela equipe

gestora do contrato.

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

4.2.4.5 Não serão concedidos acessos à rede a usuários genéricos.

4.2.4.6 Não serão concedidos acessos à rede e aos seus recursos, a usuários que não possuam vínculos formais com Poder Judiciário do Estado do Ceará, excetuados os casos devidamente justificados e autorizados pelo Comitê Gestor de Segurança da informação (CGSI).

4.2.4.7 O acesso como administrador da máquina Local só será concedido nos seguintes casos:

4.2.4.7.1 para servidores do Poder Judiciário do Estado do Ceará da área de Tecnologia da Informação, quando solicitado pelos gestores de suas respectivas áreas, com as devidas justificativas, e autorizado pelo(a) Secretário(a) de Tecnologia da Informação;

4.2.4.7.2 para usuários de empresas prestadoras de serviços de TI ou terceirizados da área de TI, quando solicitado pelos fiscais do contrato ou gestor da área de TI, com as devidas justificativas, e autorizado pelo(a) Secretário(a) de TI; e

4.2.4.7.3 para os demais casos, deverá ser solicitado ao CGSI.

4.2.4.8 A concessão ou retirada dos acessos as pastas em rede, para magistrados, servidores efetivos e comissionados, conveniados, terceirizados e estagiários do quadro ativo, serão mediantes solicitação do gestor, de acordo com a hierarquia organizacional de pastas;

4.2.4.8.1 De acordo com a hierarquia organizacional de pastas, o gestor será o proprietário da pasta de sua na hierarquia institucional ou pasta solicitada, podendo o mesmo autorizar quem poderá possuir acesso à pasta sob sua gestão;

4.2.4.8.2 Só será permitido o acesso a qualquer pasta ou arquivo no servidor, mediante registro de chamado através da Central de Atendimento de Tecnologia da Informação (CATI). O gestor deverá informar qual o nível de permissão: leitura ou alteração;

4.2.4.9 Terão direito ao uso da Rede Privada Virtual – RPV (VPN), os desembargadores, juízes, secretários do TJCE, assessores e gestores da área de Tecnologia da Informação.

4.2.4.9.1 Em casos devidamente justificados e autorizados pela Secretaria de Tecnologia da Informação, usuários poderão utilizar este recurso, desde que a solicitação seja feita pelo gestor da unidade e por prazo devidamente especificado.

4.2.5 **Sistemas de Tecnologia da Informação**

Da concessão de Acesso aos Sistemas Judiciais e Administrativos

4.2.5.1 Para a concessão ou revogação dos acessos aos Sistemas Judiciais e Administrativos para os magistrados e servidores ativos do Poder Judiciário, terceirizados contratados pela Secretaria de Gestão de Pessoas – SGP, cedidos, estagiários, deverão ser considerados os requisitos abaixo:

4.2.5.1.1 estar cadastrado no Sistema de Gerenciamento de Recursos Humanos (GRH);

4.2.5.1.2 a solicitação de acesso deverá ser realizada de acordo com os procedimentos estabelecidos pelo Gestor de Sistema na respectiva política de acesso; e

4.2.5.1.3 cessado o motivo da concessão do acesso deverá ser requerida à Secretaria de Tecnologia da Informação (Setin), a imediata desassociação do usuário do perfil.

4.2.5.1.3.1 Quando for motivado por mudança de lotação, tal requisição deverá ser feita pelo gestor da unidade de origem.

4.2.5.1.3.2 Nos demais casos, tal requisição deverá ser feita pelo gestor do usuário;

4.2.5.2 Para a concessão ou revogação dos acessos aos Sistemas Judiciais e Administrativos para os servidores/funcionários de Órgãos Públicos ou Instituições Particulares conveniados com o Poder Judiciário, deverão ser considerados os requisitos abaixo:

4.2.5.2.1 existência de cláusulas nos convênios que prevejam a concessão de acesso aos recursos de TI do Poder Judiciário do Estado do Ceará.

4.2.5.2.2 a solicitação de acesso deverá ser realizada pelo gestor da unidade de lotação de acordo com os procedimentos estabelecidos pelo Gestor de Sistema.

4.2.5.2.3 cessado o motivo da concessão do acesso, o mesmo deverá ser revogado de acordo com os termos estabelecidos no convênio e/ou na política de acesso ao sistema.

4.2.5.3 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:

4.2.5.3.1 existência de cláusulas em contratos/acordos que prevejam o acesso aos recursos de TI necessários à execução do contrato, devendo ainda constar Termo de Ciência assinado para contratos de Tecnologia da Informação.

4.2.5.3.2 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 autorizada pela equipe gestora do contrato; e

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

4.2.6 Não serão concedidos acessos aos Sistemas Judiciais e Administrativos, a usuários que não possuam vínculos formais com Poder Judiciário do Estado do Ceará, excetuados os casos devidamente justificados e autorizados pelo Gestor de Sistema ou Presidência.

Da definição dos perfis para acesso aos Sistemas Judiciais e Administrativos

4.2.7 Apenas usuários autorizados terão acesso aos recursos de sistemas.

4.2.8 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.

4.2.9 Os gestores de Sistemas Judiciais e Administrativos estabelecerão os procedimentos para a concessão e revogação dos acessos.

4.2.10 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.

4.2.11 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 do referido sistema.

5 **Competências e Responsabilidades**

5.1 **Dos Usuários/Colaboradores e dos em Regime de Exceção (Temporários)**

5.1.1 Os usuários são responsáveis pelo uso adequado dos serviços e recursos a eles atribuídos;

5.2 **Da Assistência Militar**

5.2.1 Criar procedimentos em relação aos acessos físicos as unidades e as áreas críticas, do Poder Judiciário do Estado do Ceará;

5.2.2 Criar procedimentos contra incêndios e outros desastres naturais para as áreas críticas de Tecnologia da Informação e Comunicação – TIC; e

5.2.3 Comunicar imediatamente a autoridade superior o descumprimento desta norma.

5.4 **Dos Gestores de Sistemas**

5.4.1 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.

5.5 **Dos Custodiantes da Informação**

5.5.1 **Da Área de Tecnologia da Informação**

5.5.1.1 Conceder, suspender e revogar os acessos as contas de rede e de sistemas de informações ou banco de dados conforme disposto nesta norma;

5.5.1.2 Criar e manter as contas de sistemas e serviços;

5.5.2 Disponibilizar ferramenta que permita aos gestores de unidades terem a informação dos acessos a sistemas dos usuários lotados em sua unidade.

5.5.3 Criar procedimentos para os acessos às áreas críticas de Tecnologia da Informação e Comunicação - TIC;

5.5.2 **Do Serviço de Segurança da Informação**

Promover divulgação das regras presentes do documento, acompanhar as auditorias

dos sistemas e reportar ao Comitê Gestor de Segurança da Informação as ameaças à Política de Segurança da Informação.

5.5.3 **Do Comitê Gestor de Segurança da Informação**

O comitê será acionado quando a área de Segurança da Informação julgar pertinente.

5.6 **Do Monitoramento e da Auditoria do Ambiente**

A auditoria será promovida pela respectiva área de tecnologia da informação, verificando a adoção das regras contidas no presente documento. Periodicamente, esta área remeterá relatórios para o Serviço de Segurança da Informação.

6 **Prazos e dos Controles**

6.1 A Assistência Militar deve criar procedimentos para acesso aos prédios do Poder Judiciário do Estado do Ceará **e** procedimentos contra incêndios e outros desastres naturais paras áreas críticas de Tecnologia da Informação e Comunicação- TIC**.** Os procedimentos que deverão ser inicialmente criados, estão definidos nos itens 4.1.6 e 4.1.7 e deverão ser apresentados ao Comitê Gestor de Segurança da Informação em até 90 dias após a publicação desta norma ou na próxima reunião extraordinária do CGSI.

6.2 A Assistência Militar deve informar ao CGSI qualquer necessidade de alteração nos procedimentos de acesso aos prédios deste Poder.

6.3 A Assistência Militar deve informar ao CGSI qualquer descumprimento na execução dos procedimentos de acesso aos prédios deste Poder.

6.4 A área de Tecnologia da Informação, através da gerência de infraestrutura de TI e o Serviço de Segurança da Informação deverão elaborar procedimentos para controle dos acessos às áreas críticas de TIC. Os procedimentos que deverão ser inicialmente criados, estão definidos nos itens 4.1.8 e deverão ser apresentados ao Comitê Gestor de Segurança da Informação em até 90 dias após a publicação desta norma ou na próxima reunião extraordinária do CGSI.

6.5 Por determinação da Presidência ou do CGSI qualquer acesso a qualquer tempo poderá ser revogado**;**

6.6 Prazos ou controles relativos ao controle de acesso físico ou lógico não previstos nesta norma, deverão ser encaminhados ao CGSI.

7 **Penalidades**

7.1 Uma vez que o usuário é responsável por qualquer atividade a partir de seus acessos à rede e aos sistemas, o mesmo responderá por qualquer ação legal apresentada ao Poder Judiciário do Estado do Ceará que envolva seus acessos.

7.2 No caso de evidências de uso irregular dos acessos, o usuário terá seu acesso bloqueado para averiguação.

7.3 O usuário infrator deverá ser notificado e a ocorrência de transgressão comunicada ao seu chefe imediato e à diretoria correspondente.

7.4 O acesso somente será restabelecido mediante solicitação da chefia imediata, informando que tomou conhecimento da violação das normas de segurança.

7.5 Nos casos em que ficar evidente que o usuário permitiu ou facilitou, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública, o Comitê Gestor de Segurança da Informação será informado e tomará as medidas que julgar necessárias.

7.6 As penalidades poderão incluir: bloqueio temporário, cancelamento dos acessos, processos administrativos, criminais e cíveis, além da aplicação das penalidades previstas em lei.

8 **Vigência**

8.1 Esta Norma entra em vigor na data de sua publicação.