~~Poder Judiciário do Estado de Rondônia~~
~~Secretaria de Tecnologia da Informação e Comunicação~~

Revogado pela Resolução n. 088/2019-PR

~~Política de Segurança da Informação – PSI~~

~~Biênio 2016-2017~~

~~**PRESIDENTE**~~

~~Desembargador Sansão Batista Saldanha~~

~~**VICE-PRESIDENTE**~~

~~Desembargador Isaías Fonseca Moraes~~

~~**CORREGEDOR-GERAL**~~

~~Desembargador Hiram Souza Marques~~

~~**COORDENADORA DE INFORMÁTICA**~~

~~Ângela Carmen Szymczak de Carvalho~~

~~**COMITÊ DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CGTIC)**~~

~~Desembargador Isaías Fonseca Moraes~~

~~Desembargador Valter de Oliveira~~

~~Desembargador Raduan Miguel~~

~~Juiz Auxiliar da Presidência Ilisir Bueno Rodrigues~~

~~Juiz Auxiliar da Corregedoria Danilo Augusto Kanthack Paccini~~

~~Jean Carlos Silva dos Santos~~

~~Jucélio Scheffmacher de Souza~~

~~Ângela Carmen Szymczak de Carvalho~~

~~Rosângela Vieira de Souza~~

~~Fabiano Sérgio Paiva Dias de Sá~~

~~**COMITÊ DE GESTOR DE SEGURANÇA DA INFORMAÇÃO MULTIDISCIPLINAR (CGSI)**~~

~~Desembargador Valdeci Catellar Citon~~

~~Desembargador Hiram Souza Marques~~

~~Jean Carlos Silva dos Santos~~

~~Jucélio Scheffmacher de Souza~~

~~Ângela Carmen Szymczak de Carvalho~~

~~Rosângela Vieira de Souza~~

~~Valeria de Souza Santana~~

~~Jeiele Eline Castro Silva~~

~~Rafael Silva Grangeiro~~

~~Fabiano Sérgio Paiva Dias de Sá~~

~~Ignácio de Loiola Reis Júnior~~

COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CGesTIC)

Ângela Carmen Szymczak de Carvalho

Alessandra Lima Costa

Bruno Spadeto

Fabiano de Sousa Gutierrez

Teresa Neuma Braga Leite Guimarães

Valglaci Sousa Coelho

EQUIPE DE ELABORAÇÃO

Ignácio de Loiola Reis Junior

Jorge Willians da S. Batista

Luiz Fernando Viscenheski

Thiago Fleury Marques Cotrim

Sumário

Registro de Revisões

No.	Data	Descrição da mudança	Revisor	Aprovador
1	19/11/2014	Criação do documento	Ignácio de Loiola Reis Junior	Coordenadora de Informática
2	25/08/2016	Alterações sugeridas pelo CGSI	Renata dos Santos	Presidente do Comitê Gestor de Segurança da Informação Multidisciplinar
3	14/11/2016		Ignácio de Loiola Reis Junior	Presidente do Comitê de Governança de Tecnologia da Informação e Comunicação
4	22/11/2016	Alterações sugeridas pela COPLAN e inclusão do normativo de acesso ao datacenter principal na PSI	Ignácio de Loiola Reis Junior	Tribunal Pleno

~~*Apresentação*~~

~~A Tecnologia da Informação (TI) exerce papel cada vez mais relevante para as instituições da Administração Pública. Por isso, tem crescido também a importância de se proteger as informações e os ativos de TI com relação aos riscos e às ameaças que se apresentam nesta área. Por essas razões, a segurança da informação tornou-se um ponto crucial à manutenção e ao avanço das instituições.~~

~~Ciente da relevância desse assunto, esta publicação tem o intuito de despertar a atenção para os aspectos da segurança da informação no judiciário rondoniense.~~

~~Espera-se que este trabalho possa ajudar o PJRO a aprimorar a segurança da informação, contribuindo para que a tecnologia da informação agregue ainda mais valor ao negócio da administração pública, em benefício da sociedade.~~

~~*Introdução*~~

~~Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e o uso de computadores de grande porte, a estrutura de segurança ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados. Com a chegada dos computadores pessoais e das redes de computadores, que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das instituições modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável.~~

~~O que é a Política de Segurança da Informação?~~

~~A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do PJRO para a proteção dos ativos de tecnologia da informação e comunicação, prevenção de incidentes de segurança e estabelece a responsabilidade legal de todos os usuários (colaboradores) que utilizam os serviços de tecnologia. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.~~

~~A presente PSI está baseada nas recomendações propostas pelas normas técnicas:~~

- ~~ABNT NBR 15999-1:2007;~~
- ~~ABNT ISO GUIA 73:2009;~~
- ~~ABNT NBR ISO/IEC 27001:2013;~~
- ~~ABNT NBR ISO/IEC 27002:2013;~~
- ~~ABNT NBR ISO/IEC 27005:2013;~~
- ~~ABNT NBR ISO/IEC 27001:2013.~~

~~Todas são reconhecidas mundialmente como códigos de boas práticas para a gestão da segurança da informação, bem como estão de acordo com as leis vigentes em nosso país.~~

Que assuntos devem ser abordados na PSI?

A PSI deve extrapolar o escopo abrangido pelas áreas de sistemas de informação e recursos computacionais, não sendo restrita, portanto, à área de informática. Ao contrário, ela deve estar integrada à visão, à missão, ao negócio e às metas institucionais, bem como ao plano estratégico de informática e às políticas da instituição concernentes à segurança em geral.

O conteúdo da PSI varia de instituição para instituição em função de seu estágio de maturidade, grau de informatização, área de atuação, cultura organizacional, necessidades requeridas, requisitos de segurança, entre outros aspectos.

No entanto, é comum a presença de alguns tópicos na PSI, tais como:

- Definição de segurança de informações e de sua importância como mecanismo que possibilita o compartilhamento de informações;
- Declaração do comprometimento da alta administração com a PSI, apoiando suas metas e princípios;
- Objetivos de segurança da instituição;
- Definição de responsabilidades gerais na gestão de segurança de informações;
- Orientações sobre análise e gerência de riscos;
- Princípios de conformidade dos sistemas computacionais com a PSI;
- Padrões mínimos de qualidade que esses sistemas devem possuir;
- Políticas de controle de acesso a recursos e sistemas computacionais;
- Classificação das informações (de uso irrestrito, interno, confidencial e secreto);
- Procedimentos de prevenção e detecção de vírus;
- Princípios legais que devem ser observados quanto à tecnologia da informação (direitos de propriedade de produção intelectual, direitos sobre software, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais);
- Princípios de supervisão constante das tentativas de violação da segurança de informações;

- Consequências de violações de normas estabelecidas na política de segurança;
- Princípios de gestão da continuidade do negócio;
- Plano de treinamento em segurança de informações.

Objetivos

Este documento foi elaborado pela Seção de Segurança da Informação (Sesinf), apresentado e aprovado pela Coordenadoria de Informática (Coinf), CGSI e CGTIC e aborda a Política de Segurança da Informação do Poder Judiciário do Estado de Rondônia.

O objetivo dessa Política é estabelecer diretrizes que permitam proteger o conjunto de informações e dados, no intuito de preservar o valor que possuem para o PJRO, bem como garantir os atributos essenciais de segurança (integridade, confidencialidade e disponibilidade) de todas as informações processadas pela instituição. Definem-se esses atributos como:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Aplicações da PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os usuários que utilizam recursos computacionais do PJRO.

Esta política dá ciência aos usuários de que os ambientes, sistemas, computadores e redes do PJRO poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada usuário se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Secretaria de Tecnologia da Informação e Comunicação (STIC) sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Princípios da PSI

Toda informação produzida ou recebida pelos usuários como resultado da atividade profissional contratada pelo PJRO pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos usuários para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

O PJRO, por meio da Divisão de Segurança da Informação (Disein), poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Requisitos da PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os usuários do PJRO, a fim de que a política seja cumprida.

Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê Gestor de Segurança da Informação Multidisciplinar (CGSI).

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, e sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do CGSI.

Ressalta-se que, primordialmente, todos os que necessitem ter acesso aos recursos computacionais do PJRO deverão, como requisito básico, assinar o "Termo de Responsabilidade", comprometendo-se à estrita observância e às condições e requisitos básicos para o acesso aos recursos computacionais do PJRO.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Disein e esta, se julgar necessário, deverá encaminhar posteriormente ao CGSI para análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados, no mínimo, anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação, como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas judicias, administrativos e financeiros desenvolvidos pelo PJRO ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

Das responsabilidades específicas dos usuários em geral

Entende-se por usuário qualquer pessoa que utilize algum recurso de Tecnologia da Informação e Comunicação (TIC) do Tribunal de Justiça do Estado de Rondônia, incluindo pessoas físicas ou jurídicas, podendo ser dividida em:

- Usuários internos: magistrados, servidores, estagiários, terceirizados, voluntários, que utilizam algum ativo de TIC em função de suas atribuições funcionais, e colaboradores ou prestadores de serviços, que temporariamente necessitem de acesso a algum ativo de TIC para o cumprimento de alguma prestação contratual ou atividade de interesse institucional;
- Usuários externos: jurisdicionados que utilizam serviços providos pelo Tribunal e o público em geral.

Tanto usuários internos como externos devem entender os riscos e cumprir rigorosamente o que está previsto na PSI baseado no aceite do Termo de Responsabilidade.

A concessão de acesso aos recursos de TIC poderá ser revogada a qualquer tempo se for verificado que o usuário que a recebeu não estiver cumprindo as condições definidas no aceite do Termo de Responsabilidade.

Cada usuário será responsabilizado nas esferas administrativa, cível e criminal pelo prejuízo ou dano que vier a causar ao PJRO e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Cada usuário que receber do PJRO um bem de TIC deverá utilizá-lo corretamente e de acordo com essa PSI, zelando pela sua integridade e pelo seu bom funcionamento.

Das responsabilidades específicas dos gestores de pessoas e/ou processos

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão;

- Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI do PJRO;

- Exigir dos colaboradores a assinatura do Termo de Responsabilidade, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo após o término do processo de desligamento, sobre todos os ativos de informações do PJRO;

- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

Das responsabilidades específicas da Divisão de Segurança da Informação

- Propor diretrizes que permitam proteger o conjunto de informações e dados, no sentido de preservar o valor que possuem para o PJRO, bem como garantir a integridade, confidencialidade e disponibilidade das informações processadas pela instituição;

- Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Compete à Disein:

- ~~Elaborar projetos de segurança da informação e acompanhar a sua execução;~~
- ~~Gerenciar e manter a segurança de processos (gestão de riscos do ambiente físico e lógico e elaboração de minutas de políticas de segurança);~~
- ~~Executar as Políticas de Segurança da Informação em vigência no Tribunal;~~
- ~~Coordenar a elaboração, implantação e manutenção de minutas dos planos de contingência, políticas de backup e recuperação de dados;~~
- ~~Analisar alternativas e propor a implantação de novas tecnologias de segurança para o ambiente computacional do Tribunal;~~
- ~~Auxiliar na celebração, execução e acompanhamento de contratos, convênios, acordos de cooperação ou instrumentos congêneres firmados pelo Tribunal que envolva segurança da informação;~~
- ~~Analisar criticamente incidentes em conjunto com o CGSI;~~
- ~~Promover a conscientização dos usuários em relação à relevância da segurança da informação para o negócio do PJRO, mediante campanhas, palestras, treinamentos e outros meios de marketing;~~
- ~~Realizar pesquisa científica e tecnológica na área de segurança da informação;~~
- ~~Implantar os sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede;~~
- ~~Desenvolver outras atividades inerentes a sua finalidade.~~

~~Das responsabilidades específicas do Comitê Gestor de Segurança da Informação Multidisciplinar~~

~~- Promover a cultura de Segurança da Informação, bem como estabelecer um modelo que permita a criação e a manutenção de um Sistema de Gestão de Segurança da Informação (SGSI) apoiado por uma Política de Segurança, Normas e Procedimentos.~~

Ressalta-se que o CGSI é um comitê vinculado e subordinado ao Comitê Gestor de Tecnologia da Informação e Comunicação Multidisciplinar (CGTIC). Possui natureza consultiva e de apoio, sendo de caráter permanente e tendo por finalidade analisar periodicamente a efetividade do modelo de gestão de segurança da informação implantado de forma a proporcionar melhoria contínua do PJRO.

Deve ser formalmente constituído pelos titulares das seguintes unidades do PJRO:

- Presidente do Comitê de Segurança Institucional;
- Corregedoria-Geral da Justiça;
- Secretaria Administrativa;
- Secretaria Judiciária;
- Secretaria de Tecnologia da Informação e Comunicação;
- Coordenadoria de Planejamento;
- Consultoria Jurídica;
- Diretoria do Departamento de Recursos Humanos;
- Diretoria do Departamento de Engenharia e Arquitetura;
- Assessoria de Segurança Institucional;
- Divisão de Segurança da Informação.

Cabe ao Presidente do Comitê Gestor de Segurança da Informação Multidisciplinar a coordenação dos trabalhos desenvolvidos pelo CGSI, que deverá reunir-se mensalmente. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o PJRO.

O CGSI poderá, sempre que necessário, convidar servidores e/ou colaboradores para participar das reuniões, a fim de prestar esclarecimentos.

As atividades do CGSI deverão ser executadas em conformidade com as recomendações publicadas pela Associação Brasileira de Normas Técnicas (ABNT), relativas a sistemas de gestão de segurança da informação.

Compete ao CGSI:

- Submeter ao CGTIC modelo de gestão corporativa de segurança da informação do PJRO e, se aprovado, promover sua aplicação;

- Propor à Administração do PJRO, após aprovação do CGTIC, e acompanhar estratégias, metas e ações de segurança da informação, bem como apresentar resultados decorrentes da implementação;
- Requerer às unidades do PJRO iniciativas ou informações que considerar necessárias para a implementação das estratégias, metas e ações de segurança da informação;
- Propor à Administração do PJRO, após aprovação do CGTIC, a elaboração e a revisão de políticas, normas e procedimentos inerentes à segurança da informação;
- Gerenciar e avaliar os resultados de auditorias de conformidade de segurança da informação e de aspectos legais relacionados à proteção das informações;
- Elaborar e submeter ao CGTIC proposta e atualização periódica de plano com medidas que garantam a continuidade das atividades do PJRO e o retorno à situação de normalidade em caso de desastre ou falha nos recursos que suportam os processos vitais de negócio do PJRO;
- Manifestar-se sobre ações em segurança da informação;
- Desenvolver outras atividades inerentes à sua finalidade;
- Responder as diligências relativas à segurança da informação, promovidas por meio de auditoria interna ou externa, e tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial.

Do monitoramento, auditoria e fiscalização

Para garantir as regras mencionadas nesta PSI, serão aplicados monitoramento, auditoria e fiscalização das informações pertencentes ao PJRO, com intuito de manter a disponibilidade do serviço e as atividades do PJRO.

Cabe à Disein implantar os sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado.

O responsável pela unidade poderá solicitar ao CGSI relatório contendo informações relativas a acessos de internet de seu setor, e outros pertinentes, sempre relacionadas a vulnerabilidades de segurança de informação.

A guarda e utilização das senhas de usuário administrador de domínio (Active Directory, etc.), administrador de sistema de Servidores (Linux, Windows, VMWare, etc.), Administrador de Firewall (CheckPoint, etc.), Administrador de Proxy (Websense, etc.), SA do banco de dados (Oracle, SQL, Postegre, etc.) serão de responsabilidade da equipe técnica do Tribunal de Justiça, Departamento de Serviços e Infraestrutura de TIC (Desein), sendo vedada sua disponibilização e uso por pessoas não autorizadas.

Capítulo I – Controle de acesso e gerenciamento de identidade

Este tópico tem como objetivo assegurar, por meio da gestão de identidades, privilégios e controle, o acesso aos ativos de tecnologia da informação e comunicação de usuários autorizados, e prevenir acessos não autorizados, bem como modificação, destruição ou interferência nesses ativos.

O Desein recepcionará todos os pedidos de concessão ou remoção de direito de acesso de rede, concessão de conta de e-mail institucional e pasta de compartilhamento aos serviços de TIC do PJRO por meio de registro de chamado no software Poraqui, disponível em http://poraqui/otrs/customer.pl, efetuado pelo responsável pela unidade.

O acesso aos ativos de TIC deverá ter motivação compatível com o interesse do serviço público e, em especial, com as atividades institucionais do PJRO.

Os sistemas de controle de acesso têm como premissa de segurança a proibição total de acesso aos ativos de TIC a todos os usuários, a menos que esse seja expressamente autorizado.

Os usuários internos receberão o mínimo de privilégio de acesso necessário e indispensável ao desempenho de suas atribuições funcionais e em conformidade com os interesses do PJRO, sendo vedado o fornecimento de privilégios adicionais.

Os ativos de TIC aos quais os usuários internos tiverem acesso deverão ser utilizados exclusivamente em função de suas atividades funcionais.

~~Os usuários externos poderão receber privilégio mínimo de acesso necessário e indispensável à utilização dos serviços providos pelo PJRO em meio eletrônico e de acordo com a regulamentação de cada serviço.~~

~~A identificação do usuário dar-se-á por meio de um identificador único, pessoal e intransferível, que o qualifique inequivocamente, de forma a assegurar, sempre que necessário, a sua responsabilização pelos atos praticados, sob qualquer forma, por meio dos ativos de TIC.~~

~~Os sistemas internos deverão adotar, preferencialmente, como identificador do usuário, o código de identificação do colaborador atribuído pela unidade organizacional responsável pela gestão de pessoas.~~

~~A criação de identificador de usuário destinado ao uso coletivo será permitida excepcionalmente quando destinada ao acesso de sistema ou equipamento que não enseje risco para a segurança da informação e mediante autorização explícita do CGSI. As contas de uso coletivo terão privilégios de acesso restritos ao ativo para o qual ela tenha sido criada.~~

~~O acesso aos ativos de TIC é facultado aos usuários internos e externos conforme a destinação e a regulamentação de cada ativo.~~

~~Facultar-se-á a terceiros, colaboradores ou prestadores de serviços a concessão de acesso em caráter temporário aos sistemas de uso interno mediante solicitação formal do servidor titular da unidade organizacional responsável pelas atividades do usuário, contendo, obrigatoriamente, as datas de início e de fim das atividades, acompanhada da devida justificativa, que será submetido ao Desein por meio de chamado registrado no software Poraqui. Caso essa não seja concedida, o pedido poderá ser refeito ao CGSI por meio de CI endereçada ao presidente desse comitê.~~

~~Facultar-se-á ao servidor inativo o acesso aos recursos disponibilizados na intranet que sejam relacionados ao seu cadastro, consulta de seus benefícios e proventos, ou de outras informações que o Tribunal disponibilize, de acordo com sua conveniência.~~

~~As solicitações de concessão/revogação de acesso dos usuários aos ativos de TIC, incluído o acesso aos sistemas externos providos por outras instituições, deverão~~

ser feitas formalmente pelo titular da unidade organizacional de lotação do usuário ao gestor do ativo mediante ferramenta apropriada de solicitação de serviço.

Deverá constar, na solicitação, a identificação do usuário, os ativos, os recursos e funcionalidades pretendidas e o período de validade, acompanhados de justificativa fundamentada.

A solicitação deverá ser avaliada pelo gestor do ativo, cabendo-lhe a decisão de aprová-la, total ou parcialmente.

Serão definidos e documentados pelo gestor, quando da aprovação da solicitação, os privilégios de acesso efetivamente concedidos ao usuário interessado.

A liberação do acesso ao ambiente computacional de rede far-se-á mediante assinatura do termo de responsabilidade, por meio do qual o usuário dará ciência e manifestará concordância, comprometendo-se a cumprir esta regulamentação, a Política de Segurança da Informação e outras normatizações que venham a ser dispostas sobre a segurança da informação no âmbito do PJRO.

Os termos de responsabilidade ficarão sob guarda da unidade organizacional responsável pela gestão de pessoas e deverão ser coletados, preferencialmente, na posse do colaborador.

O usuário poderá ser responsabilizado de forma administrativa, cível e criminalmente por qualquer acesso em desacordo com a presente regulamentação e, no caso de terceiros, colaboradores ou prestadores de serviços, ainda responderá, solidariamente, o titular da unidade organizacional de sua lotação, desde que comprovado conhecimento e/ou má-fé deste último.

Em se tratando de estagiários, terceirizados, voluntários, colaboradores ou prestadores de serviços, o acesso será válido pelo período de duração do estágio, contrato ou prestação de serviço, devendo ser revogado imediatamente após esse período, preferencialmente de forma automática.

Imediatamente após o encerramento do período necessário para a realização das atividades pertinentes às atribuições funcionais dos usuários, revogar-se-ão os seus direitos de acesso aos ativos de TIC.

~~Havendo mudança de lotação, atribuição, afastamento definitivo ou temporário do usuário, o Departamento de Recursos Humanos ou o Conselho da Magistratura, conforme o caso, deverá comunicar a mudança, por meio de registro de chamado no Poraqui, o mais breve possível, ao Desein, para procedimentos de ajustes ou cancelamento de credenciais de acesso, em função da adequação dos privilégios de acesso aos colaboradores.~~

~~O acesso aos ativos de TIC será precedido de um processo de autenticação no qual o usuário será identificado por meio de um identificador único. O acesso aos ativos de TIC e seus recursos ou funcionalidades dar-se-á de acordo com os privilégios de acesso do usuário, os quais serão controlados em nível adequado às funcionalidades de cada sistema.~~

~~Os servidores lotados na STIC, em razão de suas atividades de desenvolvimento, manutenção ou suporte de sistemas, poderão, excepcionalmente, ter privilégios de acesso especiais, inclusive de acesso total, de acordo com suas atribuições funcionais, mediante autorização do gestor do sistema e da chefia imediata do servidor.~~

~~O acesso direto aos dados armazenados em ambiente de produção deverá ser realizado, obrigatoriamente, através dos sistemas ou ferramentas homologadas pelo CGSI, ficando facultado à equipe de banco de dados da Divisão de Gerenciamento de Dados (Diged) o acesso às bases de dados de produção com utilização de privilégio de acesso máximo. As operações realizadas quando do acesso às bases de dados de produção por integrante da equipe de banco de dados da Diged deverão, para efeito de auditoria, ser registradas formalmente e acompanhadas da devida justificativa.~~

~~Constitui prerrogativa do titular do Desein o acesso total aos ativos de TIC, inclusive com o privilégio de conceder e revogar privilégios a outros usuários, desde que relacionados com sua atividade funcional.~~

~~Constitui prerrogativa dos gestores de ativos de TIC o acesso total aos ativos sob a sua responsabilidade, inclusive com o privilégio de conceder e revogar privilégios a outros usuários. O gestor do ativo de TIC poderá, a seu critério, delegar aos titulares das unidades organizacionais o privilégio de conceder e revogar privilégios aos usuários lotados na unidade.~~

~~Os usuários com privilégio de concessão de acesso a outros usuários deverão ser formalmente cientificados de suas responsabilidades.~~

~~Os administradores de rede, de serviços e de equipamentos deverão possuir e utilizar chaves distintas: uma para uso cotidiano e outra com privilégios de acesso especiais para as tarefas de administração, que deverá somente ser utilizada para esse fim.~~

~~Cada identificador de usuário terá uma senha correspondente, que deverá ser utilizada para autenticação quando do seu acesso aos ativos de TIC. Caberá ao usuário zelar pela confidencialidade de sua senha, que deverá ser de uso pessoal e intransferível.~~

~~A senha deverá ter nível de complexidade razoável, com quantidade mínima de oito dígitos, preferencialmente formada por números, letras e caracteres especiais, devendo-se evitar senhas de fácil dedução ou passíveis de descoberta através de ferramentas especializadas, tais quais:~~

- ~~Nomes próprios com significativo valor afetivo e de conhecimento comum, como, por exemplo, nome de familiares, animais de estimação, times de futebol e cidades; de telefone;~~
- ~~Informações pessoais fáceis de serem obtidas, como números de telefone, CPF, RG, matrículas e data de nascimento;~~
- ~~Nomes e marcas inscritas em objetos nas proximidades da estação, como o código do modelo do monitor ou da estação de trabalho;~~
- ~~Sequências ou repetições de caracteres, como 123456, abcdef, 000001;~~
- ~~Palavras contidas em dicionários de qualquer idioma.~~

~~As senhas mantidas pelos sistemas para fins de autenticação dos usuários deverão ser armazenadas, obrigatoriamente, com criptografia de nível compatível com a classificação do grau de sigilo das informações. Os sistemas já existentes e que estejam em desacordo com essa norma deverão, no prazo a ser estipulado pelo CGSI, ser adaptados de modo a se alinharem à política de segurança da informação.~~

~~O uso de senhas nos códigos fontes de programas, scripts, macros e arquivos de configuração serão permitidos quando:~~

- For empregado mecanismo de criptografia adequado para evitar a obtenção da senha por terceiros não autorizados;
- O usuário relacionado à senha utilizada tiver acesso a um conjunto restrito de dados e/ou operações sem relação com outros sistemas, e desde que não enseje risco à segurança da informação do PJRO;
- O usuário relacionado à senha utilizada tiver acesso apenas de leitura a algum dado compartilhado com outros sistemas, e desde que não enseje risco à segurança da informação do PJRO.

A critério do gestor do ativo, poderá ser exigida dos usuários a troca periódica das senhas utilizadas em ativos, de acordo com sua criticidade. A troca de senha, nos sistemas em que assim se fizer necessário, poderá ser requerida automaticamente pelos mecanismos de autenticação. Quando da alteração da senha, poderá, a critério do gestor do ativo, manter-se um histórico das últimas senhas a fim de impedir o usuário de substituir a senha por uma senha recentemente utilizada.

A distribuição de senhas iniciais deverá ser realizada de forma segura, através de meio confiável, e será sempre precedida da identificação e autenticação do usuário interessado. As senhas iniciais poderão ser distribuídas por meio de mensagens de correio eletrônico institucional enviado diretamente ao usuário. Em se tratando de senha inicial do sistema de correio eletrônico, está também poderá ser distribuída por meio de mensagens de correio eletrônico institucional destinado ao superior imediato ou ao titular da unidade organizacional de lotação do usuário. As senhas iniciais distribuídas aos usuários deverão, obrigatoriamente, ser formadas por caracteres aleatórios, não sendo permitido o uso de senhas padrões de uso rotineiro. O usuário deverá, na ocasião de seu primeiro acesso, trocar a senha inicial do ativo de TIC.

Mediante solicitação do usuário, formalmente realizada através de ferramenta apropriada, poderá a senha ser alterada pelo Desein.

Os sistemas com controle de acesso deverão permitir ao usuário a alteração de sua senha sempre que desejado.

Os mecanismos de autenticação de usuário, quando possível, deverão informar, durante o processo de autenticação, que o acesso ao ativo deverá ser realizado apenas

por usuário autorizado, bem como que ele será responsabilizado pelos atos realizados durante o período do acesso.

Quando possível, os mecanismos de autenticação de usuário deverão exibir, posteriormente à autenticação bem sucedida, o histórico dos últimos três acessos, com data, hora, identificação da estação originária e o resultado da autenticação.

Os mecanismos de autenticação de usuário não deverão exibir o identificador do último usuário logado.

Os mecanismos de autenticação de usuário, após uma tentativa de autenticação mal sucedida, não deverão indicar, individualmente, qual parte dos dados (identificador do usuário ou senha) estava incorreta. O identificador de usuário e sua respectiva senha deverão ser autenticados simultaneamente.

O mecanismo de autenticação deverá bloquear a conta do usuário, por um período não inferior a 10 (dez) minutos, a ser estipulado para cada ativo, após a quinta tentativa de autenticação sem sucesso e consecutiva em um período de até 5 (cinco) minutos. O mecanismo de autenticação poderá desbloquear automaticamente as contas de usuário após 30 (trinta) minutos do último bloqueio. O usuário poderá entrar em contato com a unidade organizacional gestora do ativo e solicitar formalmente o desbloqueio manual da conta antes de decorrido o período de bloqueio estipulado.

Os sistemas deverão, quando possível e sempre que ensejar riscos à segurança da informação, possuir mecanismos que impossibilitem que um mesmo usuário efetue acesso simultâneo a um mesmo ativo.

Os sistemas e serviços deverão, sempre que possível, utilizar a autenticação integrada com a sessão do usuário de rede em andamento, de forma a tornar transparente o processo de autenticação para usuários já autenticados no ambiente de rede.

Os serviços de rede e as novas aplicações desenvolvidas internamente ou por terceiros deverão considerar, para fins de autenticação, o uso de uma base de dados única e centralizada de usuários, preferencialmente baseada em serviço de diretório (LDAP) e/ou certificados digitais, tais como os tokens e cartões inteligentes ou o uso de biometria.

~~Os privilégios de acesso de usuários aos sistemas que assim o permitirem deverão ser mantidos em base de dados única, centralizada, baseada em um modelo de dados a ser estipulado pela STIC. A associação de privilégios e acesso a usuários deverá, sempre que possível, ser atribuída a perfis ou a grupos de usuários que executem tarefas comuns ou que tenham funções equivalentes, contemplando a segregação de funções e facilitando a operacionalização do procedimento de concessão de privilégios de acesso.~~

~~O mecanismo de autenticação deverá, sempre que transportar senhas pela rede, fazê-lo de forma segura, utilizando criptografia adequada.~~

~~Todo ambiente de TIC com acesso lógico de usuário deverá, sempre que possível, implementar mecanismo de desconexão automática (*timeout*) após período de inatividade, que não deverá ser superior a 30 (trinta) minutos.~~

~~O usuário deverá, voluntariamente, finalizar a sessão (*logoff/logout*) ou bloquear a estação sempre que for se ausentar do equipamento que estiver com uma sessão autenticada em andamento.~~

~~A qualquer momento, o Desein poderá, caso constatado o não cumprimento de qualquer dispositivo desta regulamentação ou da Política de Segurança da Informação, ou sempre que ensejar riscos à segurança, suspender imediatamente, em caráter temporário, o privilégio de acesso do usuário, sem necessidade de aviso prévio, informando, o mais breve possível, o CGSI e a chefia imediata do colaborador com acesso suspenso.~~

~~Não será permitido, salvo expressa autorização do CGSI, o uso de equipamentos ou dispositivos conectados à rede do PJRO que permitam o acesso remoto à sua rede.~~

~~Serão considerados críticos todos os equipamentos que permitam conexões externas, pelo que deverão receber tratamento apropriado para garantir a segurança do ambiente computacional do PJRO.~~

~~Todo acesso remoto destinado ao uso direto dos recursos de rede do PJRO deverá ser realizado de modo seguro, através do uso de criptografia, e preferencialmente utilizando Redes Privadas Virtuais (VPN). O acesso remoto deverá ser controlado e~~

registrado e toda comunicação externa deverá passar, obrigatoriamente, por um ponto de controle único com funcionalidades de *firewall*.

O acesso remoto deverá, obrigatoriamente, realizar-se de uma estação segura, com sistema operacional atualizado e livre de programas maliciosos. O usuário responderá por incidentes causados em função de sua negligência ou imperícia durante o acesso remoto à rede do PJRO.

Sempre que tecnicamente viável, os acessos aos serviços e sistemas deverão registrar, para efeitos de auditoria, a data e a hora do início e fim do acesso e o código de identificação do usuário, de modo a permitir o rastreamento das atividades sobre os ativos e seus recursos.

A critério do gestor do ativo de TIC, as operações que incluam, alterem ou manipulem informações de maior importância poderão ser registradas com maior grau de detalhamento para fins de auditoria. Os registros de acesso em ambientes críticos deverão ser auditados com periodicidade mínima de 2 anos, ou a qualquer tempo, mediante solicitação do CGSI.

Todos os sistemas disponibilizados em ambiente de produção deverão ser previamente homologados em ambiente apropriado, distinto, e por equipe mista composta por especialistas e usuários, designada para essa atividade, no cumprimento da política de segurança vigente no PJRO.

Todo serviço de rede não autorizado, não utilizado ou desnecessário, em estações ou servidores, que permita algum tipo de acesso através da rede e que venha oferecer algum risco à segurança da informação, deverá ser bloqueado, desabilitado ou desinstalado.

Caberá ao CGSI, com a anuência da Presidência do PJRO, esclarecer os casos omissos.

Capítulo II – Dispositivos de armazenamento

O objetivo deste tópico é definir uma metodologia para a utilização dos dispositivos de armazenamento de dados dentro do ambiente computacional do PJRO.

~~Os dispositivos de armazenamento deverão ser destinados ao armazenamento de dados estritamente relacionados às atividades institucionais do PJRO ou à função institucional do usuário que o utilizar.~~

~~Os recursos de armazenamento de dados deverão ser utilizados de forma comedida e racionalizada, devendo-se evitar o armazenamento de arquivos dispensáveis, sobretudo quando se tratar do armazenamento de dados em rede.~~

~~Os dispositivos de armazenamento deverão estar disponíveis sempre que necessário, bem como deverão possuir capacidade suficiente para armazenar toda a informação a ele destinada.~~

~~Os dispositivos de armazenamento de rede e suas áreas de dados deverão possuir controle de acesso lógico para assegurar o acesso de usuários autorizados e prevenir acessos não autorizados.~~

~~Cabe ao Desein a monitoração e o gerenciamento dos dispositivos de armazenamento de rede, o controle da capacidade e do desempenho dos dispositivos, a manutenção da estrutura de diretórios, as cópias de segurança (backup) e a elaboração e divulgação de procedimentos técnicos e melhores práticas relacionados ao uso e gestão desses recursos.~~

~~A concessão de acesso aos arquivos e diretórios de rede deverá obedecer, sem prejuízo das demais normas, ao previsto na Norma quanto ao gerenciamento de identidade e controle de acesso.~~

~~Toda unidade organizacional poderá possuir uma unidade de armazenamento na rede (diretório de rede) à sua disposição, com acesso restrito aos usuários daquela lotação e destinada ao armazenamento de arquivos estritamente relacionados às suas atividades institucionais.~~

~~O diretório de rede destinado à unidade organizacional será considerado, para fins de correição e auditoria, uma extensão daquela unidade, sendo de inteira responsabilidade do titular da unidade o seu gerenciamento e organização, devendo-se observar os seguintes procedimentos:~~

- ~~Eliminação de arquivos não inerentes às atribuições funcionais da unidade organizacional;~~

- Eliminação de arquivos duplicados;

- Eliminação de arquivos desnecessários, obsoletos ou em desuso.

O diretório de rede vinculado à unidade organizacional terá seu nome formado pela sigla daquela unidade e sua localização na estrutura de diretórios deverá refletir a posição hierárquica da unidade no âmbito do PJRO.

Os diretórios de rede vinculados às unidades organizacionais de mesma natureza terão estrutura hierárquica comuns, com nomes padronizados e conteúdo correlato com o das outras unidades que desempenhem funções institucionais análogas.

O diretório de rede vinculado à unidade organizacional terá estrutura rígida em seus níveis superiores, mais próximos à raiz, de forma a garantir a padronização da estrutura hierárquica.

A critério do responsável pela unidade organizacional poderão ser criadas novas estruturas de diretórios (subdiretórios) dentro dos respectivos diretórios de sua unidade, sendo vedada, entretanto, a criação de pastas de trabalho individuais para usuários.

Aos usuários da rede serão concedidas as permissões estritamente necessárias ao acesso aos dispositivos de armazenamentos da rede condizentes com sua lotação e atribuições funcionais.

As permissões de acesso poderão ser de leitura, de escrita e de modificação, ou uma combinação dessas.

O usuário da rede receberá permissões de acesso ao dispositivo de armazenamento da unidade em que esteja lotado, com acesso compartilhado aos arquivos dessa unidade, e com as permissões de leitura, gravação e alteração, ou de acordo com os critérios formalmente solicitados para a STIC pelo titular da unidade.

Nos casos de alteração da lotação do usuário, o Desein deverá adequar imediatamente as permissões de acesso do usuário de acordo com a solicitação de mudança formalmente encaminhada.

A solicitação de mudança caberá apenas:

- ~~Ao chefe imediato da lotação originária, o que implicará apenas a revogação dos direitos relacionados a essa lotação;~~
- ~~Ao chefe imediato da lotação de destino, o que implicará a revogação dos direitos relacionados à lotação originária e da atribuição de novos direitos de acordo com a nova lotação;~~
- ~~Ao DRH ou unidade organizacional equivalente, o que implicará a revogação dos direitos relacionados à lotação originária e da atribuição de novos direitos de acordo com a nova lotação.~~

~~O uso de dispositivos de armazenamento removíveis, tais como pendrives, cartões de memória, discos removíveis e outros similares, somente será permitido nas estações de trabalho formalmente designadas e autorizadas.~~

~~O titular de cada unidade organizacional deverá designar, de acordo com sua conveniência, as estações de trabalho referidas, ficando, ainda, responsável pelo uso de dispositivos de armazenamento removíveis nessas estações e pelos riscos decorrentes desse uso, facultando-lhe a concessão de uso aos demais usuários daquela unidade de lotação.~~

~~É vedado o armazenamento, em qualquer diretório local e, sobretudo, nos diretórios da rede, dos seguintes tipos de arquivos:~~

- ~~Imagens, áudio e vídeo de qualquer formato e cujo conteúdo não tenha relação direta com as atividades institucionais do PJRO;~~
- ~~Arquivos de qualquer natureza relacionados a programas não homologados pela Política de Segurança da Informação;~~
- ~~Programas executáveis não licenciados ou não homologados pela Política de Segurança da Informação.~~

~~Os arquivos tipificados poderão, mediante devida justificativa e autorização formal do CGSI, ser excepcionalmente armazenados na rede.~~

~~É vedado o armazenamento nos diretórios da rede de arquivos em duplicidade quando uma das cópias já esteja disponibilizada em diretório de acesso público.~~

~~A Disein poderá realizar inspeções periódicas e sem aviso prévio nos dispositivos de armazenamentos de rede para identificação de arquivos que estejam em~~

desacordo com esta norma. Os arquivos poderão ser sumariamente excluídos pela Disein sem prévio aviso aos usuários, sendo a ocorrência informada ao CGSI e ao responsável pela pasta compartilhada.

Os arquivos de imagem, áudio e vídeo, quando autorizados, deverão ser criados e armazenados utilizando, dentre outras características técnicas, padrões de codificação, compressão e resolução adequados às suas necessidades e que resultem em arquivos com tamanhos o quanto menores possíveis.

A STIC providenciará a publicação dos padrões de formato e codificação referidos nessa norma.

Capítulo III – *Backup* e restauração de dados

O objetivo desta norma é definir uma metodologia de *backup* (armazenamento) e restauração (*restore*) dos dados para o PJRO.

Todos os *backups* devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário de expediente, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os usuários responsáveis pela gestão dos sistemas de *backup* deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de *backup* (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

As fitas de *backup* devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de *backup* devem ser monitorados e controlados pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante. É necessária a previsão, em orçamento anual, da

renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de *backup* nos termos do Procedimento de Controle de Mídias de *Backup*.

As mídias de backups históricos ou especiais deverão ser armazenadas no datacenter principal, e, preferencialmente, uma cópia em ambiente seguro distinto desse.

Os *backups* imprescindíveis, críticos, para o bom funcionamento dos negócios do PJRO, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de *backup* e/ou *restore*, é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de *Backup* e *Restore*.

Quaisquer atrasos na execução de *backup* ou *restore* deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração (*restore*) de *backup* devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do *backup*.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de *backups* e *restores*, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido

pelos responsáveis e auditado pelo Diretor do Desein, nos termos do Procedimento de Controle de *Backup* e *Restore*.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

Capítulo IV – Correio eletrônico institucional

O objetivo desta norma é informar aos usuários do PJRO quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do PJRO é para fins corporativos e relacionados às atividades do usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que, feita com bom senso, não prejudique o PJRO, não cause impacto no tráfego da rede e não seja contra a ética, a moral e os bons costumes.

O e-mail institucional terá a cota de armazenamento de 200 MB (megabytes) por conta de usuário. No caso de utilização total da cota de armazenamento, o usuário ficará impossibilitado de receber e-mail.

O e-mail corporativo poderá ter um limite superior a 200 MB (megabytes), desde que devidamente justificado, por meio do sistema PORAQUI.

Os anexos das mensagens de e-mail são limitados a 20MB (megabytes), sendo automaticamente bloqueadas para envio as extensões de arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) e outras extensões comumente utilizadas por *Malwares*.

O acesso às mensagens está restrito ao remetente e ao destinatário, sendo estas invioláveis, salvo por determinação administrativa autorizada pelo CGSI, ou por motivo de segurança institucional, devendo seguir o procedimento operacional definido para essa atividade. Qualquer leitura indevida de mensagens de e-mail alheias, estará sujeita a sanções administrativas, cíveis e criminais.

São deveres e responsabilidades do usuário do e-mail institucional:

- ~~Utilizar a conta de e-mail institucional para a comunicação, em detrimento da utilização de outros serviços semelhantes;~~
- ~~Manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis;~~
- ~~Fazer o armazenamento local dos seus e-mails, para liberar espaço na sua conta, este armazenamento não fará parte da rotina de backup da STIC, portanto é de inteira responsabilidade do usuário a salvaguarda dos dados;~~
- ~~Evitar o uso do sistema de correio eletrônico para finalidades que não sejam do escopo do Poder Judiciário;~~
- ~~Não utilizar o sistema de correio eletrônico para enviar propaganda de qualquer natureza, vender qualquer objeto, mensagens festivas, mensagens indesejadas, correntes, boatos, e outros;~~
- ~~Sigilo quanto ao acesso e à guarda da credencial individual;~~
- ~~O conteúdo das mensagens e arquivos anexados enviados.~~

~~São deveres do Desein quanto ao monitoramento das contas de e-mail:~~

- ~~Configurar o correio eletrônico para enviar e-mail somente após o credenciamento do usuário;~~
- ~~Implementar medidas para filtragem de vírus e spam de e-mails indesejados (correntes, mensagens pornografias, propagandas) no sistema de correio eletrônico;~~
- ~~Implementar medidas para limitar o tamanho das caixas postais de seus usuários, definindo cotas;~~
- ~~Monitorar o funcionamento do servidor de correio eletrônico, em termos de número de conexões, número de mensagens enviadas e recebidas, número de mensagens bloqueadas, banda consumida na rede;~~
- ~~Alertar aos usuários quanto a eventual mau funcionamento ou interrupção do serviço de e-mail;~~
- ~~Alertar ao Gestor responsável quanto a eventual má utilização do e-mail por sua equipe, para as devidas providências quanto à aplicação de sanções cabíveis;~~

- Realizar a exclusão de contas de usuários desligados ou inativos, mediante solicitação da unidade competente do PJRO quanto à gestão de pessoas.

Quando se tratar de movimentação de usuário que indique desligamento definitivo com o Poder Judiciário, a chefia imediata do usuário deverá documentar a necessidade de efetuar backup dos dados privativos do usuário ao Desein, no prazo de até 60 (sessenta) dias, após o desligamento desse colaborador, por meio de CI endereçada ao CGSI, que autorizará a atividade. São considerados dados privativos do usuário aqueles armazenados em pastas de acesso exclusivo, bem como e-mails nominais enviados por membros do Poder Judiciário.

A Desein fica autorizada a excluir definitivamente o conteúdo privativo do usuário, quando decorrido o prazo estabelecido anteriormente, sem a manifestação do gestor imediato do usuário desligado.

A entrega de cópias dos arquivos e e-mails armazenados nos equipamentos do Poder Judiciário ao usuário desligado será efetuada somente mediante autorização do CGSI.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

"Nome do usuário"

E-mail: "usuário"@tjro.jus.br

"Setor do usuário"

Poder Judiciário do Estado de Rondônia

Site: www.tjro.jus.br

E-mail: "departamento"@tjro.jus.br

Telefone(s) (69) "9999"-"9999" - Ramal: "Usuário"

Capítulo V – Acesso à Internet

O objetivo desta norma é definir a utilização e o acesso à Internet.

Todas as regras atuais do PJRO visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça

~~um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.~~

~~Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita à auditoria e divulgação a chefia imediata e CGSI, para medidas cabíveis. Portanto, o PJRO, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos à internet feitos de rede e de suas dependências.~~

~~Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do PJRO, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.~~

~~O acesso à Internet, que deverá estar relacionado às atribuições do cargo ou função do usuário, será liberado desde que:~~

- ~~Não seja abusivo;~~
- ~~Não represente risco à segurança da informação;~~
- ~~Não comprometa o desempenho da rede;~~
- ~~Não influencie o bom andamento dos trabalhos.~~

~~O acesso aos seguintes sites da Internet será permitido:~~

- ~~Mecanismos de Busca (Google, Bing, Yahoo) e afins;~~
- ~~Instituições não governamentais sem fins lucrativos (*.org.br);~~
- ~~Instituições Governamentais (*.gov.br);~~
- ~~Instituições do Poder Judiciário (*.jus.br);~~
- ~~Instituições financeiras (Banco do Brasil, Caixa, HSBC) e afins.~~

~~Como é do interesse do PJRO que seus usuários estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é tolerável.~~

~~É proibida a divulgação e/ou o compartilhamento indevido de informações em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.~~

Os usuários não poderão efetuar downloads de programas não autorizados, jogos, filmes, músicas, ou qualquer outro arquivo fora do escopo institucional.

Os usuários não poderão efetuar upload (subida) de qualquer software produzido ou licenciado ao PJRO, sem a devida autorização do CGSI.

Os usuários não poderão utilizar os recursos do PJRO para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso aos seguintes sites da internet não será permitido, exceto em casos específicos para atividades relacionadas ao PJRO, com a devida autorização do CGSI:

- *Peer-to-peer* (Kazaa, BitTorrent, Morpheus, Emule, Ares) e afins;
- *Streaming* (rádios on-line, canais de broadcast) e afins;
- VoiP e Mensagem instantânea (MSN, Skype, ICQ) e afins;
- Redes sociais (Facebook, Myspace, Twitter) e afins;
- Pornográficos, racistas, ou que façam apologia ao uso de drogas e afins;
- Jogos e entretenimento e afins;
- Qualquer outro que possa ser ofensivo à moral e aos bons costumes.

É proibida a utilização de meios para burlar as políticas de bloqueios automaticamente aplicadas no *proxy* do PJRO. Tais meios envolvem *web-proxy* e tunelamentos criptografados entre outros.

Capítulo VI – Redes sociais

O objetivo desta norma é definir a utilização e manutenção do perfil institucional do PJRO nas redes sociais.

Entende-se por redes sociais ambientes virtuais que têm como objetivo reunir pessoas, empresas ou instituições, os chamados membros, que uma vez inscritos, podem expor seu perfil com dados como fotos pessoais, textos, mensagens e vídeos, além de interagir com outros membros, criando listas de amigos e comunidades.

Os Perfis institucionais mantidos nas redes sociais deverão ser administrados e gerenciados por servidores ocupantes de cargo efetivo, ou comissionados e terceirizados, sob a responsabilidade de um gestor designado pelo Presidente do PJRO.

O acesso do usuário ao seu perfil particular e/ou pessoal nas redes sociais não será permitido, exceto em casos específicos para atividades relacionadas ao PJRO, com a devida autorização do CGSI.

Capítulo VII – *Softwares*

O objetivo desta norma é definir a homologação, custódia, instalação, configuração e utilização dos softwares no âmbito do PJRO.

Está expressamente proibida a instalação e/ou a utilização de quaisquer softwares, independentemente de ser legalizado, gratuito ou apenas uma versão de avaliação, sem que tenha sido homologado e/ou autorizado pelo CGSI.

Em caráter excepcional, o CGSI poderá autorizar temporariamente a utilização de softwares não homologados para testes e avaliação.

Todos os softwares homologados pelo CGSI, relacionados às atribuições do cargo ou função do usuário, ficam disponíveis para instalação, configuração e utilização.

O privilégio de administrador local será retirado de todos os usuários para evitar instalações de softwares não homologados e configurações fora do padrão estabelecido pelo CGSI.

Em caráter excepcional, com a devida justificativa e autorização do CGSI o privilégio de administrador local será concedido.

Compete ao CGSI, amparado tecnicamente pela STIC:

- Analisar e homologar todos os softwares utilizados no âmbito do PJRO;
- Gerenciar a lista de usuários que possuem privilégio de administrador local.

A aquisição, a custódia e a disponibilização dos softwares não departamentais de uso comum no âmbito do PJRO caberão à STIC, unidade organizacional à qual também incumbirá:

- Pesquisar no mercado novos produtos que atendam às necessidades do PJRO;
- Publicação da lista dos softwares homologados pelo CGSI;

- ~~A designação, ao setor mais apropriado de sua hierarquia, ou a uma comissão por ela definida, da responsabilidade pela gestão dos softwares de uso comum homologados;~~
- ~~Providenciar a instalação, configuração e suporte dos softwares homologados;~~
- ~~Inventariar os softwares instalados nos equipamentos de informática do PJRO;~~
- ~~Desinstalar/remover softwares não homologados.~~

~~Compete ao usuário dos softwares:~~

- ~~Zelar pela correta utilização da estação de trabalho e dos softwares nela instalados, seguindo as orientações da STIC e da política de segurança da informação vigente;~~
- ~~Utilizar os softwares exclusivamente para as atividades de interesse do PJRO;~~
- ~~Acatar as normas e procedimentos operacionais para o uso de softwares;~~
- ~~Informar ao Desein eventuais inconformidades dos softwares instalados em seus equipamentos que prejudiquem o desempenho de suas atividades.~~

~~O critério de homologação de softwares deverá obedecer à Política de Segurança da Informação vigente no PJRO, aos aspectos legais de licenciamento e, ainda, à análise técnica dos seguintes aspectos:~~

- ~~Segurança;~~
- ~~Performance;~~
- ~~Impacto no ambiente computacional;~~
- ~~Custo de licenciamento e manutenção.~~

~~A homologação de programa de uso exclusivo da unidade organizacional será realizada em conjunto com o Desein, que emitirá parecer técnico. O responsável por cada unidade organizacional encaminhará formalmente essa solicitação para o CGSI por meio de CI, que cientificará a STIC sobre o processo de solicitação/aquisição.~~

~~Caberá a cada unidade organizacional interessada a aquisição, a custódia e a disponibilização dos softwares departamentais específicos e de seu uso exclusivo, bem como auxiliar e fornecer treinamento para seus colaboradores nesses programas.~~

~~Nos casos em que, por força contratual, em virtude de aquisição, renovação ou suporte de softwares, a instalação deva ser realizada por terceiros, o Desein autorizará e acompanhará integralmente o processo de instalação.~~

~~O Desein poderá utilizar mecanismos que impeçam os usuários de instalar e desinstalar softwares nas suas estações de trabalho, bem como providenciará a desinstalação dos softwares não homologados.~~

~~O usuário será responsabilizado pela execução de softwares não homologados e pelas operações executadas durante o período de execução da sessão por ele iniciada que venham a causar, mesmo que involuntariamente, danos ou prejuízos ao ambiente computacional do PJRO ou a terceiros.~~

~~Fica expressamente proibida a cessão, para benefício próprio ou de terceiros, sem autorização formal do CGSI, de cópia de software adquirido ou desenvolvido internamente.~~

~~A cópia de *softwares* adquiridos ou desenvolvidos pelo Tribunal para utilização fora do ambiente institucional somente poderá ser realizada mediante autorização formal do CGSI e desde que não viole direitos autorais ou licenciamento.~~

~~Capítulo VIII - Equipamentos de TI~~

~~O objetivo desta norma é informar aos usuários do PJRO quais são as atividades permitidas e proibidas quanto ao uso dos equipamentos de TI.~~

~~Os equipamentos disponíveis aos usuários são de propriedade do PJRO, e têm por finalidade servir e dar suporte às suas atividades institucionais, cabendo a cada usuário utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.~~

~~A STIC é responsável pela especificação, aquisição, homologação, atualização e disponibilização dos equipamentos de tecnologia da informação de uso comum necessários ao andamento dos trabalhos do PJRO.~~

~~A STIC publicará e divulgará amplamente as recomendações quanto às boas práticas no uso dos equipamentos, incluindo os requisitos de conformidade.~~

~~O inventário de componentes dos equipamentos de informática (servidores de dados, desktops e notebooks) será controlado por softwares mantido pela STIC.~~

~~É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do Desein, ou de quem este determinar. As chefias que necessitarem fazer testes e/ou modificações deverão solicitá-los previamente ao Desein.~~

~~Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.~~

~~Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o Desein mediante registro de chamado no ServiceDesk.~~

~~A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.~~

~~Arquivos pessoais e/ou não pertinentes às atividades do PJRO (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente.~~

~~Documentos imprescindíveis para as atividades dos usuários do PJRO deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.~~

Os usuários do PJRO e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da STIC.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

- Todos os computadores de uso individual deverão ter senha de *BIOS* para restringir o acesso dos usuários não autorizados. Tais senhas serão definidas pela STIC, que terá acesso a elas para manutenção dos equipamentos.
- Os usuários devem notificar imediatamente o Desein sobre qualquer ocorrência de eventos que venham a alterar o funcionamento ou que possam causar algum dano ao equipamento;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Desein ou por terceiros devidamente contratados para o serviço;
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;
- O usuário deverá manter a configuração do equipamento disponibilizado pelo PJRO, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;
- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela norma de Controle de Acesso e Gerenciamento de Identidade, todos os terminais de computador e impressoras quando não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pelo PJRO devem ter imediatamente suas senhas padrões (*default*) alteradas;
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do PJRO:

- Transportar equipamentos para qualquer outra unidade organizacional, sem a devida autorização da STIC.
- Ceder, mesmo que temporariamente, o uso a terceiros não pertencentes ao quadro funcional do Tribunal sem a devida autorização da STIC;
- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (*sniffers*);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- Utilizar software falsificado, atividade considerada delituosa de acordo com a legislação nacional.

Capítulo IX – Acesso ao Datacenter

O objetivo desta norma é regulamentar o acesso ao Datacenter do PJRO.

O Datacenter, ou Centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores e outros. Por isso, é considerado o sistema nervoso das empresas. Tem como objetivo principal garantir a disponibilidade de equipamentos que rodam sistemas cruciais para o negócio de uma organização, garantindo assim a continuidade do negócio.

O acesso ao Datacenter principal será realizado no Capítulo X. Já quanto aos localizados nas comarcas, dever-se obedecer ao seguinte regramento:

Todo acesso ao Datacenter deverá ser registrado (usuário, data e hora) mediante formulário próprio.

A lista de usuários com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede da STIC.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um funcionário autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Datacenter.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência ao Diretor do Desein, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado na presença de um colaborador do Desein.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo usuário solicitante e a autorização formal desse instrumento pelo responsável do Datacenter, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

No caso de desligamento de usuários que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão da lista de usuários autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

Capítulo X - Acesso ao Datacenter Principal

O objetivo desta norma é regulamentar o acesso ao Datacenter do PJRO. Para efeito desse normativo são estabelecidos os seguintes conceitos e definições

I – Datacenter: local onde estão concentrados os equipamentos responsáveis pelo processamento e armazenamento de dados, nos quais rodam os sistemas cruciais para o negócio da instituição;

II – Horário de funcionamento do PJRO: período compreendido entre 07h00 e 13h00 bem como entre 16h00 e 18h00 dos dias úteis;

III – Sala-Cofre: Local específico onde está localizado o Datacenter principal do Poder Judiciário do Estado de Rondônia. A Sala-Cofre, construída pelo PJRO, é um ambiente estanque, testado e certificado, que protege o Datacenter contra fogo, calor, umidade, gases corrosivos, fumaça, água, roubo, arrombamento, acesso indevido, sabotagem, impacto, pó, explosão, magnetismo e armas de fogo;

IV - O ambiente do Datacenter é composto pelas seguintes áreas: Sala UPS: Ala 1; Centro de Controle: Ala 2; Sala-Cofre: Ala 3;Corredor técnico: Ala4;

V - Autorização formal: autorização por escrito, via e-mail ou memorando.

No caso de desligamento de usuários que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão da lista de usuários autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

Em horário de funcionamento do PJRO, o acesso ao ambiente da sala-cofre somente será realizado pelas pessoas credenciadas e autorizadas pelo Desein, validada pela STIC e confirmada pelo CGSI.

São automaticamente autorizados e credenciados:

I - Presidente do CGSI;

II - Diretor do Desein;

III - Servidores lotados nas Divisões de Gerenciamento de Dados (Diged), de Infraestrutura (Dinfra) e de Segurança da Informação (Disein).

Fora do horário de funcionamento do PJRO, fins de semana e feriados, o acesso ao ambiente da sala-cofre somente será realizado para monitoramento, manutenções preventivas agendadas ou ações corretivas emergenciais, por pessoas credenciadas e autorizadas pela STIC.

~~Quando autorizado o acesso ao ambiente da sala-cofre, a liberação de acesso será feita remota ou localmente pela Divisão de Infraestrutura (Dinfra), dependendo da necessidade de acompanhamento da atividade.~~

~~As pessoas autorizadas terão livre acesso ao ambiente, desde que o façam por meio do acesso biométrico.~~

~~A STIC deverá designar as pessoas para o cadastramento biométrico nas portas de acesso à sala-cofre;~~

~~Não é permitida a entrada e ou a saída de peças, equipamentos e acessórios da sala-cofre sem o prévio conhecimento e autorização da STIC;~~

~~Não é permitida a entrada com qualquer tipo de bebida ou comida no âmbito da sala-cofre.~~

~~Todas as entradas na sala-cofre deverão ser registradas no livro de ocorrências, descrevendo o motivo da entrada e tarefas executadas em seu interior, ficando este sob guarda do Desein.~~

~~É de competência do Desein a geração de relatórios quando houver qualquer ocorrência na sala-cofre ou sempre que solicitado pela Administração do PJRO.~~

~~Serão gerados relatórios mensais apontando as ocorrências na sala-cofre, sendo encaminhados ao CGSI para conhecimento e providências (quando essas forem necessárias).~~

~~Para os casos de intervenções e serviços a serem realizados na sala-cofre pela Departamento de Engenharia e Arquitetura (DEA) da Secretária Administrativa (SA) do PJRO, o acesso também deverá seguir o mesmo fluxo de autorização e validação exposto acima.~~

~~Todos os serviços de engenharia e manutenção a serem realizados pela DEA deverão ser comunicados com antecedência prévia à STIC, sendo necessário informar o profissional que acompanhará o serviço.~~

~~Os casos omissos serão disciplinados pelo Presidente do CGTIC, mediante proposta da STIC.~~

Capítulo XI - Dispositivos móveis

O objetivo desta norma é regulamentar o uso de dispositivo móvel que utiliza os recursos computacionais do PJRO.

O PJRO deseja facilitar a mobilidade e o fluxo de informação entre seus usuários. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pelo CGSI, como: notebooks, *smartphones*, *tablets* e *pendrives*.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os usuários que utilizem tais equipamentos.

O PJRO, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O usuário, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no PJRO.

Todo usuário deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

O suporte técnico aos dispositivos móveis de propriedade do PJRO e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo usuário deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e autorização da área responsável e sem a condução, auxílio ou presença de um técnico do Desein.

O usuário deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pelo CGSI.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede de locais conhecidos pelo usuário como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do usuário, no caso de furto ou roubo de um dispositivo móvel fornecido pelo PJRO, notificar imediatamente seu gestor direto e a STIC.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O usuário deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venham causar ao PJRO e/ou a terceiros.

O usuário que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do PJRO deverá submeter previamente tais equipamentos ao processo de autorização do CGSI.

Equipamentos portáteis, como *smartphones*, *tablets*, *palmtops*, *pendrives* e *players* de qualquer espécie, quando não fornecidos ao usuário pela instituição, não serão validados para uso e conexão em sua rede corporativa.

Das punições

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas, cíveis e penais cabíveis de acordo com a infração cometida e penalidades previstas na legislação competente.

Comunicação de descumprimento

Será encaminhado ao usuário, por escrito, notificação informando o descumprimento da norma, com a indicação precisa da violação praticada, sendo também enviada uma cópia dessa para a respectiva chefia imediata.

Das disposições finais

Será encaminhado ao usuário, por escrito, notificação informando o descumprimento da norma, com a indicação precisa da violação praticada, sendo também enviada uma cópia dessa para a respectiva chefia imediata.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna PJRO. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

A Divisão de Segurança da Informação (Disein) é responsável pela elaboração de toda a documentação técnica para o cumprimento das normas de segurança de tecnologia da informação, conforme documentação técnica a ser disponibilizada:

- Procedimento de Controle de Acesso ao Datacenter;
- Procedimento de Controle de Contas Administrativas;
- Procedimento de Controle e Transferência de Equipamentos de Informática;
- Procedimento de Controle de Mídias de *Backup*;
- Procedimento de Controle de *Backup* e *Restore*;
- Termo de Responsabilidade;
- Norma de Classificação da Informação.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário, à respectiva chefia e ao CGSI. O uso de qualquer recurso para atividades ilícitas poderá acarretar ações administrativas e a penalidades decorrentes de processos civil e criminal.

Referências utilizadas

- ABNT NBR 15999-1:2007 Errata 1:2008 - Gestão de continuidade de negócios. Parte 1: Código de prática;

- ABNT ISO GUIA 73:2009 - Gestão de riscos - Vocabulário
- ISO/IEC 27035:2011 - Information technology -- Security techniques -- Information security incident management;
- ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27005:2011 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação