Revogado pela Resolução n. 350/2025

~~**PODER JUDICIÁRIO DO ESTADO DE RONDÔNIA**~~
~~**SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**~~

~~POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI~~

~~**ANEXO ÚNICO ATO N. 1111/2020-PR**~~
~~Altera o Anexo Único da Resolução n. 88/2019-PR~~

~~**Biênio 2020-2021**~~

~~PRESIDENTE~~

~~Desembargador Kyochi Mori~~

~~VICE-PRESIDENTE~~

~~Desembargadora Marialva Henriques Daldegan Bueno~~

~~CORREGEDOR-GERAL~~

~~Desembargador Valdeci Castellar Citon~~

~~SECRETÁRIO-GERAL~~

~~Juiz de Direito Rinaldo Forti da Silva~~

~~SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO~~

~~Ângela Carmen Szymczak de Carvalho~~

~~COMITÊ DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO~~

~~Desembargador Hiram Souza Marques~~

~~Desembargador José Jorge Ribeiro da Luz~~

~~Desembargadora Marialva Henriques Daldegan Bueno~~

~~Juiz Auxiliar da Presidência Guilherme Ribeiro Baldan~~

~~Juiz Auxiliar da Corregedoria Cristiano Gomes Mazzini~~

~~Elaine Piacentini Bettanin~~

~~Jucélio Scheffmacher de Souza~~

~~Ângela Carmen Szymczak de Carvalho~~

~~Rosemeire Moreira Ferreira~~

~~Fabiano Sérgio Paiva Dias de Sá~~

~~COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO MULTIDISCIPLINAR~~

~~Desembargador Daniel Ribeiro Lagos~~

~~Desembargador Valdeci Castellar Citon~~

~~Elaine Piacentini Bettanin~~

Jucélio Scheffmacher de Souza

Ângela Carmen Szymczak de Carvalho

Rosemeire Moreira Ferreira

Fabiano Sérgio Paiva Dias de Sá

Gustavo Luiz Sevegnani Nicocelli

Eduardo Luiz Will Bezerra

Ignácio de Loiola Reis Junior

COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

Simone Soares Sena de Oliveira

Alessandra Lima Costa

Reginaldo de Souza Gadelha

EQUIPE DE ELABORAÇÃO

Reginaldo de Souza Gadelha

Ignácio de Loiola Reis Junior

Jorge Willians da S. Batista

Thiago Fleury Marques Cotrim

Allan Tito Leite Ratts

Tárik Kamel de Oliveira

SUMÁRIO

REGISTRO DE REVISÕES 4

APRESENTAÇÃO 5

DISPOSIÇÕES INICIAIS 5

CAPÍTULO I - CONTROLE DE ACESSO E GERENCIAMENTO DE IDENTIDADE 6

CAPÍTULO II - USO DA VPN 12

CAPÍTULO III - DISPOSITIVOS DE ARMAZENAMENTO 13

CAPÍTULO IV - BACKUP E RESTAURAÇÃO DE DADOS 16

CAPÍTULO V - SERVIÇO DE CORREIO ELETRÔNICO INSTITUCIONAL 17

CAPÍTULO VI - ACESSO À INTERNET 21

CAPÍTULO VII - REDE Wi-Fi 23

CAPÍTULO VIII - REDES SOCIAIS 25

CAPÍTULO IX - SOFTWARES 25

CAPÍTULO X - EQUIPAMENTOS DE TIC 28

CAPÍTULO XI - ACESSO AO DATACENTER PRINCIPAL 30

CAPÍTULO XII - ACESSO AO DATACENTER DAS COMARCAS 32

CAPÍTULO XIII - DISPOSITIVOS MÓVEIS 33

DISPOSIÇÕES FINAIS 33

REFERÊNCIAS Erro! Indicador não definido.

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 Rodrigues Idalgo	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
5	–	Inclusão do Capítulo VI na PSI, *Wi Fi*	Renata dos Santos Rodrigues Idalgo	Presidente do TJRO
6	07/08/2018	Revisão e atualização da PSI	Equipe de elaboração	Comitê Gestor de Segurança da Informação Multidisciplinar
7	10/08/2018	Apresentação ao CGSI, aprovação do texto base e deliberação sobre ajustes.	Equipe de elaboração	Comitê Gestor de Segurança da Informação Multidisciplinar
8	07/10/2020	Alterações na gestão do serviço de e-mail institucional para melhor gerenciamento da disponibilidade contratual.	Equipe de elaboração	Comitê Gestor de Segurança da Informação Multidisciplinar

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 proteger as informações e os ativos de TI com relação aos riscos e as 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, essa 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.

DISPOSIÇÕES INICIAIS

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 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.

CAPÍTULO I - CONTROLE DE ACESSO E GERENCIAMENTO DE IDENTIDADE

1. O Departamento de Serviços e Infraestrutura de TIC (Desein) é a unidade responsável por receber 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 sistema de registro de chamados da STIC.

2. 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, estabelecendo se os seguintes parâmetros:

2.1. 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.

2.2. 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.

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

2.4. 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.

2.5. 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.

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

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

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

2.5.4. 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.

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

2.5.6. 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 de atendimento ao usuário. Caso essa não seja concedida, o pedido poderá ser refeito ao CGSI por meio de CI endereçada ao presidente deste Comitê.

2.5.7. 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.

2.5.8. 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.

3. 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.

3.1. Os sistemas internos deverão adotar, preferencialmente, como identificador do usuário, o cadastro do colaborador na instituição.

3.2. 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.~~

~~**4.** 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.~~

~~**5.** Serão definidos e documentados pelo gestor, quando da aprovação da solicitação, os privilégios de acesso efetivamente concedidos ao usuário interessado.~~

~~**6.** 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.~~

~~**7.** Havendo mudança de lotação, atribuição, afastamento definitivo ou temporário do usuário, a Secretaria de Gestão de Pessoas ou o Conselho da Magistratura, conforme o caso, deverá comunicar a mudança, por meio de registro de chamado no sistema de registro de chamados da STIC, 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.~~

~~**8.** 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 da chefia imediata e do gestor do sistema.~~

~~**9.** O acesso direto aos dados armazenados em ambiente de produção deverá ser realizado, obrigatoriamente, por meio 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.~~

~~9.1. 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.~~

10. 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 do usuário.

11. 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.

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

12. Os administradores de rede, de serviços e de equipamentos deverão possuir e utilizar credenciais de acesso 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.

13. 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.

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

13.1.1. Nomes próprios com significativo valor afetivo e de conhecimento comum, como, por exemplo, nome de familiares, animais de estimação, times de futebol e cidades;

13.1.2. Informações pessoais fáceis de serem obtidas, como números de telefone, CPF, RG, matrículas e data de nascimento;

13.1.3. Nomes e marcas inscritas em objetos nas proximidades da estação, como o código do modelo do monitor ou da estação de trabalho;

13.1.4. Sequências ou repetições de caracteres, como 123456, abcdef, 000001;

13.1.5. Palavras contidas em dicionários de qualquer idioma.

13.2. 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.

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

13.3.1. For empregado mecanismo de criptografia adequado para evitar a obtenção da senha por terceiros não autorizados;

13.3.2. 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;

13.3.3. 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.

14. A critério do gestor do ativo, poderá ser exigida dos usuários a troca periódica das senhas utilizadas em ativos, de acordo com sua criticidade.

14.1. A troca de senha, nos sistemas em que assim se fizer necessário, poderá ser requerida automaticamente pelos mecanismos de autenticação.

14.2. 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.

15. A distribuição de senhas iniciais deverá ser realizada de forma segura, por meio confiável, e será sempre precedida da identificação e autenticação do usuário interessado.

15.1. As senhas iniciais poderão ser distribuídas por meio de mensagens de correio eletrônico institucional enviado diretamente ao usuário.

15.2. Em se tratando de senha inicial do sistema de correio eletrônico, esta 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.

15.3. As senhas iniciais distribuídas aos usuários deverão, obrigatoriamente, ser formadas por caracteres aleatórios, não sendo permitido o uso de senhas padrões de uso rotineiro.

15.4. O usuário deverá, na ocasião de seu primeiro acesso, trocar a senha inicial do ativo de TIC.

16. Mediante solicitação formal do usuário, poderá a senha ser alterada pelo Desein.

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

18. 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.

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

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

21. O mecanismo de autenticação prover segurança contra-ataques de força bruta.

22. 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 para usuários já autenticados no ambiente de rede.

23. 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.

24. Sempre que tecnicamente viável, os acessos aos serviços e sistemas deverão registrar, para efeitos de auditoria, a data e 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.

24.1. 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.

25. 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.

26. 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.

CAPÍTULO II - USO DA VPN

27. O acesso remoto a rede de dados do PJRO será permitido em caráter excepcional e somente para fins de trabalho.

28. deverá ser realizado de modo seguro, através do uso de criptografia, e utilizando Redes Privadas Virtuais (VPN).

29. O pedido de acesso remoto deve ser formalizado junto a DESEIN, justificando a necessidade do acesso e período de uso.

30. Qualquer outro software de acesso remoto que não seja os disponibilizado ou que não estejam devidamente homologados pela DESESIN são proibidos.

31. O acesso remoto deve ser concedido por um período de tempo pré-definido

32. A Divisão de Segurança da Informação deve definir e informar aos usuários os requisitos mínimos de segurança estabelecidos para realização de acesso remoto.

33. Quando os recursos de informática forem de propriedade de terceiros, a Divisão de Segurança da Informação deve solicitar a estes que os referidos recursos atendam aos requisitos mínimos de segurança estipulados.

34. A DESEIN deve registrar e monitorar o acesso remoto do usuário.

CAPÍTULO III - DISPOSITIVOS DE ARMAZENAMENTO

35. 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.

36. Os dispositivos 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.

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

38. Os dispositivos de armazenamento de rede e suas áreas de dados deverão possuir controle que impeça o acesso não autorizado

39. Não será permitido o compartilhamento de uma pasta local de um computador em rede, optando-se pela utilização e pastas compartilhadas no servidor e arquivos do PJRO, objetivando a garantia da inclusão dos dados na rotina de backup, garantindo a continuidade do negócio.

40. Cabe ao Desein o monitoramento 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.

41. A concessão de acesso ao sistema de arquivos da rede de rede deverá obedecer, sem prejuízo das demais normas, aos aqui previstos quanto ao gerenciamento de identidade e controle de acesso.

42. 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.

42.1. 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:

42.1.1. Eliminação de arquivos não inerentes às atribuições funcionais da unidade organizacional;

42.1.2. Eliminação de arquivos duplicados; e

42.1.3. Eliminação de arquivos desnecessários, obsoletos ou em desuso.

42.2. 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.

42.3. 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.

42.4. 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.

42.5. A critério do responsável pela unidade organizacional poderão ser criadas novas estruturas de diretórios (subdiretórios) dentro dos respectivos diretórios de sua unidade.

43. 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.

43.1. As permissões de acesso poderão ser de leitura, de escrita e de modificação, ou uma combinação dessas de acordo com os critérios formalmente solicitados para a STIC pelo titular da unidade.

43.2. O usuário da rede receberá permissões de acesso ao dispositivo de armazenamento da unidade em que esteja lotado, com acesso compartilhado aos arquivos desta unidade.

43.3. 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.

43.4. A solicitação de mudança caberá apenas:

43.4.1. Ao chefe imediato da lotação originária, o que implicará apenas a revogação dos direitos relacionados a essa lotação;

43.4.2. 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;

43.4.3. À Secretaria de Gestão de Pessoas/SGP 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.

44. 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.

44.1. 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.

45. É vedado o armazenamento em repositórios de dados disponibilizados pelo PJRO, dos seguintes tipos de arquivos não relacionados ao desempenho de atividades deste Tribunal:

45.1. Imagens, áudio e vídeo de qualquer formato e cujo conteúdo não tenha relação direta com as atividades institucionais do PJRO;

45.2. Arquivos de qualquer natureza relacionados a programas não homologados pela Política de Segurança da Informação;

45.3. Programas executáveis não licenciados ou não homologados pela Política de Segurança da Informação.

45.4. Arquivos em duplicidade, quando uma das cópias já esteja disponibilizada em diretório de acesso público;

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

45.6. 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 do menor tamanho possível.

46. 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.

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

CAPÍTULO IV - BACKUP E RESTAURAÇÃO DE DADOS

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

49. As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser devidamente identificadas e acondicionadas em local seco, climatizado e seguro (de preferência em cofres corta-fogo) segundo as normas da ABNT.

50. 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 na gravação ou 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.

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

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

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

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

53.1. 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.

53.2. 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.

53.3. 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.

54. 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.

55. 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 V - SERVIÇO DE CORREIO ELETRÔNICO INSTITUCIONAL

56. O uso do serviço de correio eletrônico do PJRO é para fins corporativos e relacionados às atividades do usuário dentro da instituição.

57. O serviço de correio eletrônico só será considerado corporativo para o domínio @tjro.jus.br, mensagens enviadas por outro domínio não serão aceitos como mensagens oficiais.

58. As solicitações de criação, alteração e exclusão de caixas postais devem ser encaminhadas à STIC - Secretaria de Tecnologia da Informação e Comunicação.

Da Caixa Postal Institucional - Pessoal

59. Todo magistrado/servidor poderá ter uma caixa postal institucional pessoal.

60. É vedada a criação de conta de e-mail corporativo para prestadores de serviço.

61. A SGP - Secretaria de Gestão de Pessoas e o DECOM - Departamento do Conselho da Magistratura nos casos de falecimento, aposentadoria, cedência a outro órgão, retorno à origem, desligamento, demissão ou exoneração, deverão

comunicar imediatamente à STIC - Secretaria de Tecnologia da Informação e Comunicação.

62. De posse do relatório que trata o item 61, incumbe à STIC - Secretaria de Tecnologia da Informação e Comunicação:

62.1. Excluir definitivamente a caixa postal no prazo de até 30 dias, após realização de backup;

63. Contas de e-mail inativas por tempo superior a 3 (três) meses, devem ser desativadas mediante informação ao magistrado/servidor, e após o decorrer de 30 (trinta) dias podem ser excluídas definitivamente, desde que realizado o procedimento de backup.

64. Os prazos de desativação e exclusão de contas de correio eletrônico podem ser reduzidos pontualmente mediante autorização do Comitê de Gestor de Segurança Multidisciplinar.

64.2 Não se aplicam os prazos de do 62 e 63 às contas de correio eletrônico que jamais fizeram login na ferramenta, sendo consideradas como não existentes, portanto, para quaisquer efeitos, de livre exclusão pela DESEIN. Inclusive, sem a necessidade de informação ao magistrado/servidor, ou mesmo, de realização de backup.

Da Caixa Postal Institucional - Estagiário

65. O gestor da unidade poderá solicitar, por escrito, a criação de caixa postal institucional pessoa ao estagiário somente quando houver essa necessidade para o serviço a ser desempenhado.

66. O uso do correio eletrônico pelo estagiário autorizado será de responsabilidade do gestor da unidade a que estiver vinculado.

67. Após a comunicação da SGP - Secretaria de Gestão de Pessoas sobre o término do estágio, a caixa postal institucional do estagiário será excluída definitivamente, mediante realização de backup.

Da Caixa Postal Institucional - Unidade

68. As unidades administrativas e judiciárias previstas na estrutura organizacional do Tribunal poderão ter caixa postal institucional da unidade.

69. O gestor da unidade será também o gestor da respectiva caixa postal, competindo-lhe:

69.1. Solicitar a criação, a alteração e a exclusão da caixa postal institucional da unidade.

69.2. Autorizar o acesso de outros servidores, mediante delegação no sistema de correio eletrônico, bem como excluir esse acesso.

70. A caixa postal institucional da unidade terá um único endereço de correio eletrônico, cujo identificador será formado pela denominação da unidade ou por sigla que permita a sua identificação.

71. A caixa postal institucional da unidade terá um único endereço de correio eletrônico, cujo identificador será formado pela denominação da unidade ou por sigla que permita a sua identificação.

72. Nessa hipótese, quando da solicitação de criação da caixa postal, deverão ser indicados o magistrado, servidor ou unidade que será responsável pelo respectivo gerenciamento, bem como, se for o caso, o período em que a caixa postal deverá ser mantida.

Da Lista de Distribuição (criação, alteração e exclusão)

73. É permitida a criação de lista de distribuição, com o objetivo de facilitar e otimizar a troca de informações sobre assuntos de interesse do Tribunal.

74. A criação de lista de distribuição pode ser solicitada pelo gestor da unidade a qual se destina ou pela Presidência.

75. A solicitação deve ser encaminhada à STIC - Secretaria de Tecnologia da Informação e Comunicações, acompanhada de justificativa e de informações sobre a finalidade da lista, nome do gestor da lista, e, quando destinada à atividade temporária, do período de sua duração.

76. Cada lista de distribuição terá um gestor, a quem incumbe:

76.1. Manter permanentemente atualizado o rol de integrantes da lista de distribuição;

76.2. Solicitar exclusão como gestor e indicar, simultaneamente, o novo responsável pela lista de distribuição;

76.3. Solicitar exclusão da lista de distribuição, quando esta não for mais necessária.

77. O identificador do endereço eletrônico será formado pela denominação ou sigla, que permita, de forma clara, a identificação de sua finalidade, ou do grupo de endereços eletrônicos nela reunidos, seguido da palavra “lista”, separados por hífen.

Disposições Gerais

78. 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.

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

79.1. Utilizar a conta de e-mail institucional para a comunicação, em detrimento da utilização de outros serviços semelhantes;

79.2. Evitar o uso do sistema de correio eletrônico para finalidades que não sejam do escopo do Poder Judiciário;

79.3. Sigilo quanto ao acesso e à guarda da credencial individual;

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

80.1. Alertar aos usuários quanto a eventual mau funcionamento ou interrupção do serviço de e-mail;

80.2. 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;

81. 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.

82. As mensagens de correio eletrônico deverão preferencialmente, incluir assinatura, conforme sugestão a seguir:

82.1. Exemplo:

"Nome do usuário"
"Setor do usuário"
Poder Judiciário do Estado de Rondônia
Telefone(s)/Ramal (69) "9999"-"9999"

Do Monitoramento e Auditoria do Serviço de Correio Eletrônico

83. O uso do correio eletrônico será monitorado por meio de ferramentas com o intuito de impedir o recebimento de *spam, hoax, phishing*, mensagens contendo vírus e outros arquivos que coloquem em risco a segurança da infraestrutura tecnológica do PJRO ou que contenham conteúdo impróprio.

84. As auditorias serão coordenadas pela DISEIN - Divisão de Segurança da Informação e os relatórios serão encaminhados ao CGSI - Comitê Gestor de Segurança da Informação.

85. As auditorias deverão ser precedidas de autorização do CGSI - Comitê Gestor de Segurança da Informação.

86. Os arquivos de registro de mensagens eletrônicas (logs) serão mantidos pelo prazo de 5 anos, exceto nos casos de auditoria ou notificação administrativa ou judicial, em que serão devidamente armazenados pela DISEIN - Divisão de Segurança da Informação, por meio de backup, a fim de salvaguardar os dados respectivos.

87. A STIC - Secretaria de Tecnologia da Informação e Comunicações encaminhará, até o dia 5 de dezembro de cada ano, relatório às unidades e aos respectivos gestores, com o rol das listas de distribuição e caixas postais a elas vinculadas, bem como a lista de eventuais caixas postais de estagiários lotados na respectiva unidade.

88. Cabe ao gestor conferir os dados do relatório referido no item anterior e, até o dia 15 de dezembro do mesmo ano, fazer os ajustes necessários.

CAPÍTULO VI - ACESSO À INTERNET

89. O acesso à internet dar-se-á, exclusivamente, pelos meios autorizados, configurados pela Secretaria de Tecnologia da Informação e Comunicações.

90. Todo tráfego de internet será controlado e inspecionado, de forma automática, pela ferramenta de proxy (filtro de conteúdo), configurada de acordo com os limites estabelecidos por esta norma ou definidos pela Administração do Tribunal.

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

91.1. Não seja abusivo;

91.2. Não represente risco à segurança da informação;

91.3. Não comprometa o desempenho da rede;

91.4. Não influencie o bom andamento dos trabalhos.

92. 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.

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

94. É proibido 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.

95. Constitui acesso indevido à internet exceto em casos específicos com a devida autorização do CGSI qualquer das seguintes ações:

95.1. Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a política de segurança da informação, tais como pornografia, pedofilia, racismo, jogos, páginas de distribuição e de compartilhamento de software e peer to peer;

95.2. Acessar sítios que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade da rede do PJRO;

95.3. Acessar ou fazer download de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo

95.4. 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.

96. Cabe ao gestor da unidade orientar os usuários sob sua responsabilidade a respeito do uso adequado do recurso de internet, conforme as regras estabelecidas nesta resolução, bem como reportar a Divisão de Segurança da da Informação ou Comitê de Segurança da Informação o seu descumprimento.

97. A critério do CGSI, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à internet, seja em situações normais de funcionamento, seja em situações de contingência, tais como:

97.1. Bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios e serviços; e

97.2. Limitação de banda de tráfego de dados.

98. As medidas identificadas no item anterior, quando implementadas, serão comunicadas à Divisão de Suporte aos Usuários, a fim de possibilitar o repasse de informações aos usuários interessados.

99. Por motivos de segurança, todo acesso à internet será monitorado, e os registros serão mantidos pela Secretaria de Tecnologia da Informação e Comunicações.

100. Em caso de indícios de descumprimento das diretrizes previstas neste capítulo, a chefia imediata ou superior solicitará, justificadamente, ao Comitê de Segurança da Informação a realização de auditoria extraordinária.

101. Os relatórios decorrentes das auditorias ordinárias e extraordinárias realizadas pelo Divisão de Segurança da Informação serão encaminhados ao Comitê de Segurança da Informação, para os devidos fins.

CAPÍTULO VII - REDE *Wi-Fi*

102. As redes Wi-Fi Corporativas são definidas através de SSIDs (Service Set Identification) com as seguintes nomenclaturas:

102.1. PJRO – Rede destinada a funcionários e magistrados do PJRO na capital e no interior é uma extensão da rede cabeada, disponível para os notebooks e equipamentos de propriedade do PJRO.

102.2. PJRO Móvel – Rede destinada aos dispositivos móveis particulares dos servidores e magistrados do PJRO, para ter acesso à internet utilizando o mesmo usuário e senha da rede cabeada.

102.3. PJRO Visitante – Rede com tempo de acesso pré-definido destinada aos advogados e a população em geral, permitindo o acesso à Internet, sem acesso à rede corporativa do PJRO. Deverá ser realizado um cadastro no momento em que se conectar à rede WI FI informando nome, CPF e e-mail.

102.4. MPRO – Rede destinada a atender ao convênio entre Ministério Público e Tribunal de Justiça, sem acesso à rede corporativa do PJRO, com acesso à rede corporativa do MPRO e a internet para atender as necessidades dos promotores.

103. A criação de SSID's para atendimento de demandas provisórias ou temporárias dependerá da aprovação do CGSI ou determinação da Presidência do PJRO.

104. O acesso à rede sem fio estará disponível 24h por dia, exceto para a rede "PJRO Visitante", que funcionará durante a semana das 7h às 18h, estando

~~indisponível aos sábados, domingos e feriados. Os horários de disponibilidade das redes poderão sofrer alterações de acordo com a conveniência do PJRO.~~

~~**105.** Cabe à STIC orientar os usuários sobre o uso adequado da rede wireless, podendo prestar auxílio ao usuário visitante que não consiga conectar seu dispositivo móvel à internet sem fio do PJRO. No entanto, não prestará suporte técnico de hardware ou software, configuração, manutenção dos equipamentos e instalação ou desinstalação de softwares.~~

~~**106.** Cabe a Discin - Divisão de Segurança da Informação analisar os incidentes de segurança da informação, bem como recomendar ações corretivas e preventivas, podendo intervir e interromper acessos nas seguintes situações:~~

~~106.1. Quando for infringida qualquer lei ou regulamento local, estadual, nacional ou internacional aplicável;~~

~~106.2. Acessar, mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;~~

~~106.3. Utilizar os recursos computacionais do PJRO para fins comerciais ou políticos, tais como mala direta, spams ou propaganda política;~~

~~106.4. Atividades que comprometam os recursos computacionais da rede do PJRO, tais como, consumo excessivo de link da internet devido à existência de programas maliciosos nos dispositivos móveis, (vírus, spyware, worm, outros);~~

~~106.5. Violar ou tentar violar os sistemas de segurança, quebrando ou tentando adivinhar a identidade eletrônica de outro usuário, senhas ou outros dispositivos de segurança;~~

~~106.6. Atividades que promovam a corrupção ou destruição de dados de usuários;~~

~~106.7. Atividades que interrompam ou prejudiquem a utilização dos serviços de rede por outros usuários;~~

~~106.8. Utilizar os recursos computacionais do PJRO para constranger, assediar, ameaçar ou perseguir qualquer pessoa;~~

~~106.9. Efetuar ou tentar efetuar qualquer tipo de acesso não autorizado aos recursos computacionais do PJRO;~~

~~106.10. Utilizar os recursos computacionais do PJRO para invadir, alterar ou destruir recursos computacionais de outras instituições;~~

~~106.11. Interceptar ou tentar interceptar a transmissão de dados através de monitoração;~~

106.12. Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando o congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais do PJRO; e

106.13. Compartilhar sua identidade eletrônica, senha ou outro dispositivo de segurança, revelando-os a terceiros.

107. A Disein deverá informar ao CGSI sobre os incidentes de segurança e as medidas tomadas, para que o CGSI tome as providências cabíveis.

108. Todos os dispositivos do usuário final ou sistemas que se conectem à rede sem fio do PJRO, devem respeitar as mesmas políticas, procedimentos e práticas que regulam o uso e o funcionamento de qualquer dispositivo ou sistema conectado à rede corporativa do PJRO;

109. O uso da internet está vinculado à conta de usuário e seu respectivo dispositivo de acesso à rede wireless. Caso constem acessos indevidos, ou inapropriados, os usuários serão notificados e poderão ter seu acesso e dispositivo bloqueados sendo responsabilizado por qualquer dano causado à rede corporativa do PJRO;

CAPÍTULO VIII - REDES SOCIAIS

110. Os perfis institucionais do PJRO nas redes sociais serão de responsabilidade do titular responsável pela Comunicação Social.

111. O acesso do servidor a redes sociais está permitido naquelas em que o Poder Judiciário do Estado de Rondônia está presente, para divulgação e marketing, e excepcionalmente as que o CGSI permitir.

112. A chefia imediata poderá solicitar o bloqueio ao acesso de redes sociais, por parte de seus servidores, desde que de maneira justificada, ao Presidente do CGSI, que pode solicitar relatórios técnicos para subsidiar sua decisão.

CAPÍTULO IX - SOFTWARES

113. É 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.

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

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

116. 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.

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

117. Compete ao CGSI, amparado tecnicamente pela STIC:

117.1. Analisar e homologar todos os softwares utilizados no âmbito do PJRO;

117.2. Gerenciar a lista de usuários que possuem privilégio de administrador local.

118. 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:

118.1. Pesquisar no mercado novos produtos que atendam às necessidades do PJRO;

118.2. Publicação da lista dos softwares homologados pelo CGSI;

118.3. 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;

118.4. Providenciar a instalação, configuração e suporte dos softwares homologados;

118.5. Inventariar os softwares instalados nos equipamentos de informática do PJRO;

118.6. Desinstalar/remover softwares não homologados.

119. Compete ao usuário dos softwares:

119.1. 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;

119.2. Utilizar os softwares exclusivamente para as atividades de interesse do PJRO;

119.3. Acatar as normas e procedimentos operacionais para o uso de softwares;

119.4. Informar ao Desein eventuais inconformidades dos softwares instalados em seus equipamentos que prejudiquem o desempenho de suas atividades.

120. O Processo de 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:

120.1. Segurança;

120.2. Performance;

120.3. Impacto no ambiente computacional;

120.4. Custo de licenciamento e manutenção.

121. A homologação de programa de uso exclusivo da unidade organizacional é de responsabilidade do Desein, que emitirá parecer técnico sempre que solicitada a implementação de aplicação ainda não homologada.

122. Caberá a cada unidade organizacional interessada na 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

123. A Homologação de Software de Terceiros oriundo de licitação deverá ser realizada como parte do procedimento de Recebimento do Objeto, desde que constados no instrumento editalício os requisitos e parâmetros formais.

124. 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.

125. 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.

126. 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.

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

128. 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 X - EQUIPAMENTOS DE TIC

129. 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.

130. 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.

131. 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.

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

133. O inventário de ativos de TIC será controlado por softwares mantido pela STIC e que qualquer solicitação de relatório personalizado deverá ser feito pelo responsável da unidade mediante registro de chamado no sistema de atendimento ao usuário instituído, que será submetido ao CGSI.

134. 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.

135. 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 sistema de Atendimento ao usuário instituído.

136. 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.

137. Os usuários do PJRO e/ou detentores de contas privilegiadas não devem executar comandos ou programas que venham sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da STIC.

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

138.1. 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.

138.2. 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;

138.3. É expressamente proibido o consumo de alimentos, bebidas e fumo na mesa de trabalho e próximo aos equipamentos;

138.4. 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;

138.5. 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;

138.6. Todos os recursos tecnológicos adquiridos pelo PJRO devem ter imediatamente suas senhas padrões (default) alteradas;

138.7. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

139. É proibido o uso de computadores e recursos tecnológicos do PJRO nas seguintes situações:

139.1. Transportar equipamentos para qualquer outra unidade organizacional, sem a devida autorização da STIC.

139.2. Ceder, mesmo que temporariamente, o uso a terceiros não pertencentes ao quadro funcional do Tribunal sem a devida autorização da STIC;
139.3. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
139.4. Burlar quaisquer sistemas de segurança;
139.5. Acessar informações confidenciais sem explícita autorização do proprietário;
139.6. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
139.7. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
139.8. 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;
139.9. Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral e a ordem pública;
139.10. Utilizar software falsificado, atividade considerada delituosa de acordo com a legislação nacional.

CAPÍTULO XI - ACESSO AO DATACENTER PRINCIPAL

140. Para efeito deste capítulo são estabelecidos os seguintes conceitos e definições:
140.1. 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.
140.2. Horário de funcionamento do PJRO: período compreendido entre 07h00 e 13h00 bem como entre 16h00 e 18h00 dos dias úteis;
140.3. Sala-Cofre: Local específico onde está localizado o Datacenter principal do Poder Judiciário do Estado de Rondônia. A Sala-Cofre, é um ambiente estanque, testado e certificado, que protege o Datacenter contra fogo, calor, umidade, gases

corrosivos, fumaça, alagamentos, roubo, arrombamento, acesso indevido, sabotagem, impacto, pó, explosão, magnetismo e armas de fogo;

140.4. 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;

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

141. 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.

142. 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.

142.1. São automaticamente autorizados e credenciados:

142.1.1. Presidente do CGSI;

142.1.2. Diretor do Desein;

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

143. 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.

144. 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.

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

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

146. 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;

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

148. 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.

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

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

151. Para os casos de intervenções e serviços a serem realizados nos edifícios que impactem no funcionamento dos Data Centers, a STIC deve ser notificada.

CAPÍTULO XII - ACESSO AO DATACENTER DAS COMARCAS

152. O acesso ao Datacenter principal é regulamentado no Capítulo XI. Já quanto aos localizados nas comarcas, deve-se obedecer ao seguinte regramento:

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

152.2. 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.

152.3. 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.

152.4. 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.

152.5. 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.

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

152.7. 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 deste instrumento pelo responsável do Datacenter, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

152.8. 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 XIII - DISPOSITIVOS MÓVEIS

153. 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

154. 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).

155. 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.

156. 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.

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

DISPOSIÇÕES FINAIS

157. Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do PJRO. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética da instituição.

158. 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:

158.1. Procedimento de Controle de Acesso ao Datacenter;

158.2. Procedimento de Controle de Contas Administrativas;

158.3. Procedimento de Controle de Mídias de Backup;

158.4. Procedimento de Controle de Backup e Restore;

158.5. Norma de Classificação da Informação.

159. 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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - **ABNT. NBR 22313** Segurança da sociedade – Sistemas de gestão de continuidade de negócios – Orientações

_____. NBR **ISO/IEC 27005:2011**: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.

_____. **NBR ISO/IEC 27001:2013:** Tecnologia da Informação – Técnicas de segurança — Sistemas de Gestão da segurança da informação - Requisitos. Rio de Janeiro, 2013.

_____. **NBR ISO/IEC 27002:2013:** Tecnologia da Informação – Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION – ISO. **ISO/IEC 27035:2011**: Information technology -- Security techniques -- Information security

~~incident management;~~