ANEXO I

RESOLUÇÃO N. 350/2025-TJRO

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

REGRAS DE SIGILO E CONFIDENCIALIDADE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA (PSIC)

JUNHO/2025

PRESIDENTE
Desembargador Raduan Miguel Filho

VICE-PRESIDENTE
Desembargador Glodner Luiz Pauletto

CORREGEDOR-GERAL
Desembargador Gilberto Barbosa Batista dos Santos

SECRETÁRIO GERAL
Juiz Rinaldo Forti Silva

SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Ângela Carmen Szymczak de Carvalho

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO MULTIDISCIPLINAR
Desembargador Glodner Luiz Pauletto
Desembargador Gilberto Barbosa Batista dos Santos
Juíza Valdirene Alves da Fonseca Clementele
Elaine Piacentini Bettanin
Jucélio Scheffmacher de Souza
Ângela Carmen Szymczak de Carvalho
Rosemeire Moreira Ferreira
Fabiano Sergio Paiva Dias de Sá
Gustavo Luiz Sevagnan Nicocelli
Eduardo Luiz Will Bezerra
Reginaldo de Souza Gadelha
Ignácio de Loiola Reis Junior
Hilton José de Santana Pinto

COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho
Alessandra Lima Costa
Reginaldo de Souza Gadelha
Simone Soares Sena de Oliveira

EQUIPE DE ELABORAÇÃO

Allan Tito Leite Ratts
Ângela Carmen Szymczak de Carvalho
Fernanda Soares Lana
Ignacio de Loiola Reis Junior
Jorge Willians da Silva Ferreira Batista
Reginaldo de Souza Gadelha
Sidnei Roberto Feliciano da Silva
Simone Soares Sena de Oliveira
Tárik Kamel de Oliveira
Thiago Fleury Marques Cotrim

1. OBJETIVO

Estabelecer diretrizes e padrões de comportamento para resguardar o sigilo e a confidencialidade das informações classificadas com grau de sigilo no âmbito do Poder Judiciário do Estado de Rondônia - PJRO.

2. MOTIVAÇÃO

Para o bom e fiel desempenho das atividades do PJRO, é necessário o conhecimento e a disponibilização de informações classificadas com grau de sigilo, incluídas aquelas referentes a processos, documentos, sistemas e qualquer outro tipo de dado. Tais informações devem ser protegidas com sigilo e confidencialidade, em consonância com a Política de Segurança da Informação Cibernética (PSIC), inclusive no que diz respeito às regras definidas neste Anexo.

3. DAS DEFINIÇÕES

3.1. Todas as informações obtidas em razão do exercício das atribuições do cargo ou função no TJRO devem ser preservadas e mantidas sob reserva, sendo consideradas reservadas ou confidenciais, por serem classificadas com grau de sigilo.

3.2. Serão consideradas, para efeitos deste Anexo, todas e quaisquer informações de natureza técnica, operacional, comercial, jurídica, *know-how*, além de processos, planos, métodos, técnicas, experiências acumuladas, documentos, contratos, papéis, estudos, pareceres, análises, pesquisas ou qualquer outro dado a que o servidor(a) ou outro(a) colaborador(a) do TJRO tenha acesso:

3.2.1. Por meio físico ou eletrônico, como: documentos expressos, manuscritos, fac-símile, mensagens eletrônicas (e-mail), imagens, processos, entre outros.

3.2.2. Por forma registrada ou armazenada em mídia digital, como: disquete, CD-ROM, DVD, HD externo, pendrive, entre outros.

3.2.3. Por meio oral, inclusive em reuniões, atendimentos ou comunicações autorizadas, conforme a legislação aplicável.

4. DA RESPONSABILIDADE

4.1. É dever do(a) servidor(a) e colaborador(a) do TJRO manter sigilo absoluto sobre as informações restritas ou sigilosas, sendo vedado utilizá-las em benefício próprio ou de terceiros.

4.1.1. As informações confidenciais, reservadas ou sigilosas confiadas ao(à) servidor(a) ou colaborador(a) do TJRO, somente poderão ser compartilhadas com terceiros mediante consentimento prévio e por escrito da unidade competente ou por determinação judicial, hipótese em que deverá ser comunicada, por escrito e de imediato, à chefia imediata.

5. DAS INFORMAÇÕES NÃO CONFIDENCIAIS

5.1. Não configuram informações confidenciais aquelas:

5.1.1. Já disponíveis ao público em geral sem classificação de sigilo.

5.1.2. Que já eram do conhecimento dos demais servidores(as) e outros(as) colaboradores(as) do TJRO antes de seu ingresso na Instituição.

5.1.3. Que não são mais tratadas com restrição pelo TJRO.

6. DA GUARDA DAS INFORMAÇÕES

6.1. Todas as informações com grau de sigilo previstas neste Anexo terão validade durante toda a vigência deste instrumento, enquanto perdurar a relação de trabalho e, ainda, por tempo indeterminado, após a perda do vínculo com o TJRO.

7. DAS OBRIGAÇÕES

7.1. Os(as) servidores(as) e demais colaboradores(as) do TJRO deverão:

7.1.1. Usar as informações apenas com o propósito de bem e fielmente cumprir os fins e interesses institucionais do TJRO.

7.1.2. Manter o sigilo relativo às informações confidenciais e revelá-las apenas a colaboradores ou outras pessoas autorizadas com necessidade de acesso.

7.1.3. Proteger as informações confidenciais que lhe foram divulgadas, usando o mesmo grau de cuidado utilizado para proteger suas próprias informações confidenciais.

7.1.4. Manter procedimentos administrativos adequados à prevenção de extravio ou perda de quaisquer documentos ou informações confidenciais, devendo comunicar à chefia imediata, em ato contínuo, a ocorrência de incidentes desta natureza, o que não excluirá sua responsabilidade.

7.2. O(A) servidor(a)/colaborador(a) do TJRO fica desde já proibido(a) de produzir cópias ou backup, por qualquer meio ou forma, de qualquer dos documentos a ele fornecidos ou que tenham chegado ao seu conhecimento em virtude da relação do exercício da função.

7.3. O(A) servidor(a)/colaborador(a) do TJRO deverá devolver, íntegros e integralmente, todos os documentos a ele fornecidos, inclusive as cópias porventura necessárias, quando não for mais necessária a manutenção das informações confidenciais, comprometendo-se a não reter quaisquer reproduções, cópias ou segundas vias, sob pena de incorrer nas responsabilidades previstas neste instrumento.

7.4. O(A) servidor(a)/colaborador(a) do TJRO deverá destruir todo e qualquer documento por ele produzido que contenha informações confidenciais relativas ao trabalho, mesmo que a título de rascunho ou similar, quando não mais for necessária a manutenção dessas informações, comprometendo-se a não reter quaisquer reproduções, sob pena de incorrer nas responsabilidades previstas neste instrumento.

8. DAS DISPOSIÇÕES ESPECIAIS

8.1. Todas as condições, termos e obrigações ora constituídas serão regidas pelo presente Anexo, pela Política de Segurança da Informação Cibernética (PSIC) do PJRO e pela legislação e regulamentação brasileiras pertinentes.

8.2. As alterações do número, natureza e quantidade das informações confidenciais disponibilizadas pelo TJRO não descaracterizarão ou reduzirão o compromisso ou as obrigações previstas neste Anexo, que permanecerá válido e com todos os seus efeitos legais em qualquer das situações tipificadas neste instrumento.

8.3. O acréscimo, complementação, substituição ou esclarecimento de qualquer das informações confidenciais disponibilizadas ao(à) servidor(a) ou colaborador(a) do TJRO receberá a mesma proteção conferida às informações originalmente disponibilizadas.

9. RESPONSABILIDADES DE SEGURANÇA DA INFORMAÇÃO

9.1. Ao utilizar os recursos computacionais do ambiente tecnológico do PJRO, o(a) servidor(a)/colaborador(a) do TJRO sujeita-se às responsabilidades inerentes às suas atribuições, devendo:

9.1.1. Acessar os sistemas informatizados somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na legislação.

9.1.2. Não revelar as informações confidenciais, reservadas ou sigilosas que lhe forem confiadas, e que somente poderão ser abertas a terceiro mediante consentimento prévio e por escrito do responsável pelo setor de Segurança da Informação do PJRO ou em caso de determinação judicial, hipótese em que deve informar de imediato, por escrito, ao seu superior hierárquico.

9.1.3. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas.

9.1.4. Para garantir a impossibilidade de acesso indevido por terceiros, não deverá se ausentar do terminal sem encerrar ou bloquear a sessão do sistema.

9.1.5. Não revelar as suas senhas de login da rede e de acesso aos sistemas a ninguém e seguir as recomendações de segurança em relação à criação de uma senha forte, conforme política vigente, de forma a possibilitar que ela continue secreta.

9.1.6. Responder, em todas as instâncias, pelas consequências das ações ou omissões de sua parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de sua senha ou das transações e informações a que tenha acesso.

9.1.7. Não disponibilizar ou fornecer informações classificadas com grau de sigilo, incluídas aquelas referentes a processos, documentos, sistemas e qualquer outro tipo de dado, aos quais tenha conhecimento.

9.1.8. Todas as informações com grau de sigilo previstas neste Anexo terão validade durante toda a vigência deste instrumento, enquanto perdurar a relação de trabalho e, ainda, por tempo indeterminado, após a perda do vínculo com o TJRO.

9.1.9. Manter procedimentos administrativos adequados à prevenção de extravio ou perda de quaisquer documentos ou informações confidenciais, devendo comunicar à chefia imediata, em ato contínuo, a ocorrência de incidentes desta natureza, o que não excluirá sua responsabilidade.

9.1.10. Manter estrita observância à Política de Segurança da Informação Cibernética (PSIC) do PJRO.

9.1.11. 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 Cibernética e outras normatizações que venham a ser dispostas sobre a segurança cibernética no âmbito do PJRO.

9.1.12. É responsabilidade do(a) servidor(a) ou colaborador(a) do TJRO cuidar da integridade, confidencialidade e disponibilidade dos dados, informações e sistemas aos quais tem acesso, devendo comunicar, por escrito, à chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou de falhas identificadas nos sistemas, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes.

9.1.13. O acesso à informação não garante ao(à) servidor(a)/colaborador(a) do TJRO direito sobre ela, nem lhe confere autoridade para liberar acesso a outras pessoas.

9.1.14. O descumprimento das disposições deste Anexo caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo da responsabilidade criminal e civil.

9.1.15. O acesso aos sistemas de dados para fins escusos ou imotivados, constitui, sem prejuízo das cominações legais, infração funcional grave, pela qual o(a) servidor(a)/colaborador(a) poderá ser responsabilizado por culpa ou dolo, acerca dos prejuízos que vier causar ao TJRO ou a terceiros.

9.1.16. Constitui descumprimento de normas e regulamentos a quebra de sigilo funcional, a divulgação de dados obtidos dos sistemas informatizados ou quaisquer outras informações pertinentes ao PJRO a que o(a) servidor(a)/colaborador(a) tenha conhecimento decorrente por força de suas atribuições.

9.1.17. Ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração de revelação de sigilo funcional do qual tenha se apropriado em razão do cargo, e crime contra a administração pública, sujeitando-se o infrator à punição de demissão, conforme tipificado no art. 170, inciso VII, da Lei Complementar n. 68, de 09/12/1992 (Regime Jurídico dos Servidores Públicos Civis do Estado de Rondônia), e às penas pelo cometimento de crime contra a administração pública, tipificado no art. 325, do Decreto-Lei n. 2.848, de 07/12/1940 - Código Penal e sua atualização através da Lei n. 9.983 de 14/07/2000, a divulgação, a quem não tenha a devida autorização, de informações dos sistemas fazendários ou quaisquer outras informações pertinentes, protegidas pelo sigilo fiscal, sujeitando o(a) infrator(a) à penalidade de demissão.

9.1.18. Sem prejuízo da responsabilidade criminal e civil e de outras infrações disciplinares, constitui falta de zelo e dedicação às atribuições do cargo, bem como do descumprimento de normas legais e regulamentares, não proceder com o devido cuidado na guarda e utilização de senha ou emprestá-la a outro colaborador, ainda que habilitado (observar o § 1º do art. 325 do Código Penal).

9.1.19. Constitui infração funcional inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados nos sistemas informatizados ou bancos de dados da Administração Pública, bem como modificar ou alterar o sistema de informações ou programas de informática sem autorização ou solicitação de autoridade competente, sujeitando o infrator à punição de demissão, conforme tipificado no art. 170, inciso I, da Lei Complementar n. 68, de 09/12/1992 (Regime Jurídico dos Servidores Públicos Civis do Estado de Rondônia), e às penas pelo cometimento de crime contra a administração pública, tipificado no Código Penal Brasileiro e suas atualizações (art. 313 – A e art. 313 - B da Lei n. 9.983 de 14/07/2000).

9.1.20. O(A) servidor(a)/colaborador(a) do TJRO deve prestar estrita obediência ao disposto na Política de Segurança da Informação Cibernética (PSIC) do PJRO, bem como manter-se ciente de suas atualizações, que serão devidamente homologadas e publicadas no site do PJRO, submetendo-se, em caso de descumprimento, às penalidades administrativas previstas nos normativos do PJRO e demais legislação aplicável, sem prejuízo da responsabilidade criminal e civil.

9.1.21. Todas as condições e obrigações ora constituídas serão regidas pela Política de Segurança da Informação Cibernética (PSIC) do PJRO, bem como pela legislação e regulamentação brasileiras pertinentes.

10. DAS PENALIDADES

10.1. A não observância de quaisquer das disposições de confidencialidade estabelecidas neste instrumento sujeitará o(a) servidor(a) ou colaborador(a) do TJRO infrator(a), bem

como o(a) agente causador(a) ou facilitador(a), por ação ou omissão, à responsabilização civil, criminal e administrativa, a ser apurada em processo judicial ou administrativo regular.

ANEXO II

RESOLUÇÃO N. 350/2025-TJRO

TERMO DE CIÊNCIA E COMPROMISSO COM A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA (PSIC)

TERMO DE CIÊNCIA E COMPROMISSO COM A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	
NOME	
CPF	
Declaro estar ciente e comprometo-me a observar e cumprir a Política de Segurança da Informação Cibernética (PSIC) do Poder Judiciário do Estado de Rondônia, instituída pela Resolução n. 350/2025-TJRO, incluindo seus Anexos, bem como as regras de sigilo e confidencialidade e demais normativos sobre segurança cibernética vigentes no âmbito do PJRO.	
Local - UF	
Data	
_____ **Assinatura**	

ANEXO III

RESOLUÇÃO N. 350/2025-TJRO

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

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA (PSIC)

NORMA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA

NSIC 01 - GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO AOS RECURSOS DE TIC

PRESIDENTE
Desembargador Raduan Miguel Filho

VICE-PRESIDENTE
Desembargador Glodner Luiz Pauletto

CORREGEDOR-GERAL
Desembargador Gilberto Barbosa Batista dos Santos

SECRETÁRIO GERAL
Juiz Rinaldo Forti Silva

SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO MULTIDISCIPLINAR

Desembargador Glodner Luiz Pauletto

Desembargador Gilberto Barbosa Batista dos Santos

Juíza Valdirene Alves da Fonseca Clementele

Elaine Piacentini Bettanin

Jucélio Scheffmacher de Souza

Ângela Carmen Szymczak de Carvalho

Rosemeire Moreira Ferreira

Fabiano Sergio Paiva Dias de Sá

Gustavo Luiz Sevagnan Nicocelli

Eduardo Luiz Will Bezerra

Reginaldo de Souza Gadelha

Ignácio de Loiola Reis Junior

Hilton José de Santana Pinto

COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

Alessandra Lima Costa

Reginaldo de Souza Gadelha

Simone Soares Sena de Oliveira

EQUIPE DE ELABORAÇÃO

Allan Tito Leite Ratts

Ângela Carmen Szymczak de Carvalho

Fernanda Soares Lana

Ignacio de Loiola Reis Junior

Jorge Willians da Silva Ferreira Batista

Reginaldo de Souza Gadelha

Sidnei Roberto Feliciano da Silva
Simone Soares Sena de Oliveira
Tárik Kamel de Oliveira
Thiago Fleury Marques Cotrim

REGISTRO DE REVISÕES

Política de Segurança da Informação (PSI)				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	novembro/2014	Criação da política.	Sesinf	Coinf
2	janeiro/2017	Acréscimo de critérios para acessar o datacenter principal. Formalizada por meio da Resolução n. 036/2016, republicada em 2017 por erro material.	DISEIN DIESE	Tribunal Pleno
3	abril/2019	Atualização da Política. Formalizada por meio da Resolução n. 088/2019.	DISEIN DIESE	CGSI
4	novembro/2020	Alteração na gestão do serviço de correio eletrônico institucional. Formalizada por meio do Ato n. 1.111/2020.	DESEIN DISEIN DIESE	CGSI
5	junho/2021	Atualização sobre a atuação do Comitê Permanente de Segurança do Poder Judiciário. Formalizada por meio da Resolução n. 209/2021.	DESEIN DISEIN DIESE	CGSI
Política da Segurança da Informação Cibernética (PSIC) **NSIC 01 - Gestão de identidade e controle de acesso aos recursos de TIC**				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**

1	junho/2025	Alteração na Resolução para focar na segurança da informação cibernética e criação de anexos específicos para tratar cada tema individualmente.	DESEIN DISEIN DIESE	Cgestic CGSI

1 OBJETIVO

Estabelecer diretrizes e padrões para gestão de identidade e controle de acesso ao uso de recursos de TIC no âmbito do Poder Judiciário do Estado de Rondônia (PJRO).

2 MOTIVAÇÃO

2.1 Disciplinar o Controle de Acesso e Gerenciamento de Identidade por meio da conscientização

2.2 Proteção da Confidencialidade, Integridade, Disponibilidade e Autenticidade das Informações do Poder Judiciário do Estado de Rondônia.

3 REFERÊNCIAS E FUNDAMENTAÇÃO LEGAL

3.1 Norma Técnica ABNT NBR ISO/IEC 27001:2022, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da Organização.

3.2 Norma Técnica ABNT NBR ISO/IEC 27002:2022, que fornece diretrizes para práticas de gestão de segurança da informação.

3.3 Portaria n. 162/2021-CNJ, que aprova Protocolos e Manuais criados pela Resolução n. 396/2021-CNJ, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

3.4 Lei Geral de Proteção de Dados (LGPD) - Lei n. 13.709/2018, que estabelece regras para o tratamento de dados pessoais, garantindo a privacidade e a proteção das informações, especialmente relevantes no contexto judiciário.

3.5 Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011, que regulamenta o acesso a informações públicas, reforçando a importância da segurança na gestão e divulgação dessas informações.

4 GLOSSÁRIO

4.1 **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

4.2 **Ativo**: qualquer coisa que tenha valor para a organização, material ou não;

4.3 **Serviço de TIC:** serviço fornecido pela área da Tecnologia da Informação e Comunicação. O gerenciamento de serviços de TIC é composto de uma combinação de tecnologia, pessoas e processos. Um serviço é um meio de entregar valor, facilitando os resultados que os clientes desejam alcançar.

4.4 **Ativos de TIC:** conjunto dos ativos de informação, ativos de rede, processos, funcionalidades e recursos de software e serviços de TIC.

4.5 **Controle de Acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra e requer procedimentos de autenticação.

4.6 **Software de Gerenciamento de Serviço de TIC (ITSM):** Sistema para registro e gerenciamento das solicitações de serviços de TIC. Atualmente no PJRO é utilizada a ferramenta Por Aqui.

4.7 **Gestor do Ativo:** pessoa(s) responsável(is) pela autorização/negação de acesso em um ativo de TIC, que esteja sob sua gerência.

4.8 **Usuário:** pessoa ou sistema que recebeu direito de acesso aos ativos de TIC do PJRO.

4.9 **Usuário Externo:** pessoa que não é servidor ou magistrado do PJRO, sistema não desenvolvido ou suportado pelo PJRO.

4.10 **Confidencialidade**: princípio que a informação esteja indisponível ou não revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada.

4.11 **Integridade**: princípio que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

4.12 **Disponibilidade**: princípio que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

4.13 **Autenticidade**: propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

4.14 **TJRO**: Tribunal de Justiça de Rondônia

4.15 **SGP**: Secretaria de Gestão de Pessoas

4.16 **PJRO**: Poder Judiciário do Estado de Rondônia

4.17 **DIGED**: Divisão de gerenciamento de dados

4.18 **GPTIR**: Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética

4.19 **CGSI**: Comitê Gestor de Segurança da Informação e Cibernética Multidisciplinar

5 CONTROLES

Seção I

Da concessão ou remoção de acesso

5.1 A STIC é a unidade responsável por receber os pedidos de concessão ou remoção de direito de acesso de rede, concessão de conta de correio eletrônico 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.

5.2 O acesso aos ativos de TIC deverá atender os seguintes parâmetros:

5.2.1 Motivação compatível com o interesse do serviço público e, em especial, com as atividades e interesses institucionais do PJRO.

5.2.2 Proibição total de acesso aos ativos de TIC por padrão, a menos que seja expressamente autorizado.

5.2.3 Os usuários internos receberão exatamente o nível de acesso indispensável e exclusivamente em conformidade com o desempenho de suas atribuições funcionais, adotando-se o princípio do privilégio mínimo de acesso.

5.2.4 Os usuários externos receberão o privilégio mínimo indispensável à utilização dos serviços providos pelo PJRO em meio eletrônico, conforme regulamentação de cada serviço.

5.2.5 As solicitações de concessão/revogação de acesso, incluído o acesso aos sistemas nacionais 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 gerenciamento de serviços de TIC.

5.2.5.1 São requisitos da solicitação: identificação do usuário; os ativos ou recursos e funcionalidades pretendidas; período de validade e justificativa fundamentada.

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

5.2.5.3 O gestor definirá os privilégios de acesso que serão concedidos ao usuário interessado e os documentará no momento da aprovação da solicitação.

5.2.5.4 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 Cibernética e outras normatizações que venham a ser dispostas sobre a segurança cibernética no âmbito do PJRO.

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

5.2.5.6 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.

5.2.5.7 Facultar-se-á a concessão de acesso em caráter temporário aos sistemas de uso interno à terceiros, colaboradores ou prestadores de serviço, mediante solicitação do servidor titular da unidade organizacional responsável pelas atividades do usuário, devendo:

5.2.5.7.1 Conter a identificação do usuário, período de validade do acesso e justificativa documentada;

5.2.5.7.2 Submeter via chamado no Sistema de Gerenciamento de Serviços de TIC a solicitação para a STIC;

5.2.5.7.3 Em caso de negação do acesso, requerer diretamente ao CGSI por meio de protocolo SEI endereçado ao Presidente do CGSI;

5.2.5.7.4 Acesso liberado somente no período de duração do estágio, contrato ou prestação de serviço, com revogação preferencialmente de maneira automática;

Seção II

Da identificação e autenticidade do acesso

5.3 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.

5.3.1 Os sistemas internos deverão adotar, preferencialmente, como identificador do usuário, a matrícula do colaborador na instituição.

5.3.2 É vedada a criação de identificador de usuário destinado ao uso coletivo.

5.4 Facultar-se-á o acesso aos recursos disponibilizados na intranet que sejam relacionados ao cadastro, consulta de benefícios e proventos, ou de outras informações aos(às) magistrados(as) e servidores(as) inativos(as), de acordo com a conveniência do TJRO.

5.5 O usuário poderá ser responsabilizado de forma administrativa, cível e criminalmente por qualquer acesso em desacordo com a presente regulamentação.

5.6 Compete aos setores e às chefias responsáveis comunicar à STIC, por meio de chamado no Sistema de Gerenciamento de Serviços, com a maior brevidade possível, conforme detalhamento a seguir:

5.6.1 À SGP e ao Departamento do Conselho da Magistratura, nos casos de afastamento temporário ou definitivo de usuária ou usuário, para realização dos ajustes ou cancelamento das credenciais de acesso, conforme a adequação dos privilégios.

5.6.2 À chefia imediata, em caso de mudança de lotação, para suspensão dos acessos aos sistemas organizacionais da unidade de origem.

5.6.3 À chefia da nova unidade de lotação, compete solicitar os novos perfis de acesso necessários.

Seção III

Da concessão de acesso privilegiado

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

5.8 O acesso direto aos dados armazenados nos ambientes de banco de dados deverão ser realizado, obrigatoriamente, por meio dos sistemas ou ferramentas homologadas pelo CGSI, com a devida autorização por meio formal do gestor negocial do(s) sistema(s) que geram tal informação, onde a equipe de gerenciamento de banco de dados concederá o acesso de acordo com o nível necessário para a operação/consulta requerida aos dados.

5.8.1 As operações realizadas quando do acesso às bases de dados de produção serão passíveis de auditoria, e tais operações deverão ser formalmente registradas e acompanhadas da devida justificativa.

5.8.2 As aplicações que acessam as bases de dados do TJRO, deverão ter usuários únicos e específicos para o acesso necessário, sendo de uso exclusivo das mesmas.

5.8.3 O usuário de acesso às bases de dados do TJRO, que não seja de aplicação, deverá ser vinculado à pessoa responsável para uso privativo, este usuário será passível de auditoria das operações na base de dados.

5.9 O titular da STIC tem a prerrogativa de acesso total aos ativos de TIC e pode conceder e revogar privilégios a outros usuários.

5.10 Os gestores de ativos de TIC tem a prerrogativa de acesso total aos ativos sob sua responsabilidade e podem conceder e revogar privilégios a outros usuários.

5.10.1 O gestor de 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.

5.10.2 Os usuários com privilégio de concessão de acesso deverão ser formalmente cientificados de suas responsabilidades.

5.11 Os administradores de rede, de serviços e de equipamentos deverão possuir e utilizar uma credencial específica e exclusiva para os acessos especiais voltados às tarefas de administração dos ativos de TIC.

Seção IV

Dos requisitos de segurança para o acesso

5.12 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 e respeitar os seguintes critérios de segurança:

5.12.1 A senha deverá ter nível de complexidade razoável, com quantidade mínima de 08 (oito) dígitos, obrigatoriamente formada por números, letras maiúsculas e minúsculas e caracteres especiais, devendo-se evitar senhas de fácil dedução ou passíveis de descoberta através de ferramentas especializadas, tais quais:

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

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

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

5.12.1.4 Sequências ou repetições de caracteres, como por exemplo, 123456, abcdef, 000001;

5.12.1.5 Palavras contidas em dicionários de qualquer idioma.

5.12.2 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.

5.12.2.1 Os sistemas existentes que estão em desacordo com essa política deverão ser adaptados, no prazo a ser estipulado pelo CGSI.

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

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

5.12.3.2 O usuário vinculado 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 cibernética do PJRO;

5.12.3.3 O usuário vinculado à senha utilizada tiver acesso apenas de leitura a algum dado compartilhado com outros sistemas;

5.12.3.4 As permissões especificadas no item 5.12.3 serão autorizadas somente se não apresentarem risco à segurança cibernética do PJRO.

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

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

5.13.2 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.

5.13.3 A senhas de identificação do usuário do Active Directory (AD) terão validade de 90 (noventa) dias, após esse período a mesma será expirada automaticamente pelo sistema.

5.13.3.1 As senhas expiradas poderão ser trocadas na estação de trabalho no Tribunal ou através do link https://trocadesenha.tjro.jus.br.

5.13.3.2 A STIC deverá enviar correio eletrônico informando sobre a expiração da senha do AD, 30 (trinta) dias, 15 (quinze) dias e 7 (sete) dias antes de a expiração ocorrer.

5.14 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.

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

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

5.14.3 O usuário deverá, na ocasião de seu primeiro acesso, trocar a senha inicial.

5.15 Mediante solicitação formal do usuário, poderá a STIC:

5.15.1 Criar uma senha temporária que será enviada para o correio eletrônico pessoal e institucional do usuário, previamente cadastrado;

5.15.1.1 O usuário deverá alterar a senha no primeiro acesso;

5.15.1.2 A senha temporária será gerada automaticamente pelo sistema, garantindo sua confidencialidade;

5.15.1.3 A senha temporária terá validade de 8 (oito) horas;

5.15.2 Solicitar a troca de senha de forma presencial, nos casos em que não for possível executar as medidas anteriores ou não sendo possível a identificação do usuário;

5.15.3 A senha em hipótese alguma deverá ser repassada via telefone.

Seção V
Dos mecanismos de controle e autenticação

5.16 Os sistemas com controle de acesso permitirão a alteração da senha sempre que o usuário desejar.

5.17 Os sistemas com controle de acesso deverão obrigatoriamente utilizar MFA (autenticação multifator), adicionando uma camada de proteção ao processo de entrada.

5.17.1 Os usuários deverão fornecer uma verificação de identidade adicional ao acessar contas ou aplicativos, como a leitura de impressão digital ou adição de código verificador.

5.17.2 Nos casos em que a autenticação multifator (MFA) for perdida, o recadastramento do dispositivo utilizado para o MFA deverá ser feito preferencialmente de forma presencial.

5.17.2.1 Diante da impossibilidade de comparecer presencialmente, deverá ser utilizada ferramenta de videochamada que possibilite a autenticação segura da identidade do usuário.

5.18 Os mecanismos de autenticação de usuário deverão oferecer as seguintes medidas de segurança:

5.18.1 Não deverão exibir o identificador do último usuário logado.

5.18.2 Após uma tentativa de autenticação malsucedida, não deverão indicar separadamente qual parte dos dados (identificador do usuário ou senha) estava incorreta.

5.18.3 O identificador de usuário e sua respectiva senha deverão ser autenticados simultaneamente.

5.18.4 O mecanismo deverá prover segurança contra-ataques de força bruta.

5.18.5 Após 5 (cinco) tentativas de login malsucedida o usuário ficará com seu cadastro bloqueado por 15 (quinze) minutos.

5.19 Os sistemas e serviços deverão utilizar a autenticação integrada com a sessão do usuário de rede em andamento, sempre que possível.

5.20 Para uso de serviços de rede e as novas aplicações desenvolvidas internamente ou por terceiros deverá ser usada 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.

5.21 Para efeitos de auditoria deverão ser registrados:

5.21.1 Informações dos acessos aos serviços e sistemas como 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, sempre que tecnicamente viável;

5.21.2 As operações que incluam, alterem ou manipulem informações de maior importância poderão ser registradas com maior grau de detalhamento, conforme critério do gestor do ativo de TIC;

5.21.3 Os registros de acesso em ambientes críticos deverão ser auditados com periodicidade mínima de 2 anos, ou a qualquer tempo, mediante solicitação do CGSI.

5.22 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 cibernética deverá ser bloqueado, desabilitado ou desinstalado.

5.23 O uso da internet está vinculado à conta do usuário e seu respectivo dispositivo de acesso à rede Wi-Fi. Caso constem acessos indevidos, ou inapropriados, o usuário será notificado e poderá ter seu acesso e dispositivo bloqueado, além de ser responsabilizado por qualquer dano causado às redes do PJRO.

6 MONITORAMENTO E AUDITORIA

6.1 Por motivos de segurança, todos os acessos serão monitorados e os registros serão mantidos pela Secretaria de Tecnologia da Informação e Comunicação por no mínimo 6 (seis) meses e até 12 (doze) meses.

6.2 Em caso de indícios de descumprimento das diretrizes previstas neste normativo, o Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética poderá de ofício ou por determinação do CGSI realizar auditoria sobre os fatos.

6.3 Os relatórios decorrentes das auditorias ordinárias e extraordinárias realizadas pelo Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética serão encaminhados ao CGSI, para análise e deliberação.

7 DISPOSIÇÃO FINAL

7.1 O disposto na presente norma será atualizado sempre que alterados os procedimentos e controles ou quando necessário, mediante iniciativa do CGSI.

ANEXO IV

RESOLUÇÃO N. 350/2025-TJRO

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

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA (PSIC)

NORMA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA

NSIC 02 - CONTROLE DE ACESSO À INTERNET

PRESIDENTE
Desembargador Raduan Miguel Filho

VICE-PRESIDENTE
Desembargador Glodner Luiz Pauletto

CORREGEDOR-GERAL
Desembargador Gilberto Barbosa Batista dos Santos

SECRETÁRIO GERAL
Juiz Rinaldo Forti Silva

SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Ângela Carmen Szymczak de Carvalho

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO MULTIDISCIPLINAR
Desembargador Glodner Luiz Pauletto
Desembargador Gilberto Barbosa Batista dos Santos
Juíza Valdirene Alves da Fonseca Clementele
Elaine Piacentini Bettanin
Jucélio Scheffmacher de Souza
Ângela Carmen Szymczak de Carvalho
Rosemeire Moreira Ferreira
Fabiano Sergio Paiva Dias de Sá
Gustavo Luiz Sevagnan Nicocelli
Eduardo Luiz Will Bezerra
Reginaldo de Souza Gadelha
Ignácio de Loiola Reis Junior
Hilton José de Santana Pinto

COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho
Alessandra Lima Costa
Reginaldo de Souza Gadelha
Simone Soares Sena de Oliveira

EQUIPE DE ELABORAÇÃO

Allan Tito Leite Ratts
Ângela Carmen Szymczak de Carvalho
Fernanda Soares Lana
Ignacio de Loiola Reis Junior
Jorge Willians da Silva Ferreira Batista
Reginaldo de Souza Gadelha
Sidnei Roberto Feliciano da Silva
Simone Soares Sena de Oliveira
Tárik Kamel de Oliveira
Thiago Fleury Marques Cotrim

REGISTRO DE REVISÕES

Política de Segurança da Informação (PSI)				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	novembro/2014	Criação da política.	Sesinf	Coinf
2	janeiro/2017	Acréscimo de critérios para acessar o datacenter principal. Formalizada por meio da Resolução n. 036/2016, republicada em 2017 por erro material.	DISEIN DIESE	Tribunal Pleno
3	abril/2019	Atualização da Política. Formalizada por meio da Resolução n. 088/2019.	DISEIN DIESE	CGSI

4	novembro/2020	Alteração na gestão do serviço de correio eletrônico institucional. Formalizada por meio do Ato n. 1.111/2020.	DESEIN DISEIN DIESE	CGSI
5	junho/2021	Atualização sobre a atuação do Comitê Permanente de Segurança do Poder Judiciário. Formalizada por meio da Resolução n. 209/2021.	DESEIN DISEIN DIESE	CGSI

Política da Segurança da Informação Cibernética (PSIC) **NSIC 02 - Controle de Acesso à Internet**				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	junho/2025	Alteração na Resolução para focar na segurança da informação cibernética e criação de anexos específicos para tratar cada tema individualmente.	DESEIN DISEIN DIESE	Cgestic CGSI

1 OBJETIVO

Estabelecer diretrizes, padrões e boas práticas de segurança cibernética para o acesso à Internet no âmbito do Poder Judiciário do Estado de Rondônia, com o objetivo de garantir a proteção da confidencialidade, integridade, disponibilidade e autenticidade das informações.

2 MOTIVAÇÃO

2.1 Disciplinar, por meio da conscientização e controles, o uso aceitável do acesso à Internet, promovendo a resiliência cibernética do Poder Judiciário e a proteção da sua reputação diante de ameaças emergentes.

2.2 Assegurar a conscientização cibernética entre os colaboradores, fomentando a compreensão dos riscos e a adoção de comportamentos seguros, visando não apenas a proteção das informações, mas também a confiança dos cidadãos e demais partes interessadas.

2.3 Garantir a proteção contra ameaças internas e externas, fortalecendo a postura de segurança cibernética do Poder Judiciário e mitigando potenciais riscos à integridade das informações.

2.4 Reforçar o compromisso com a responsabilidade institucional, demonstrando a importância da norma no tratamento ético e seguro das informações, fortalecendo a confiança da sociedade no sistema judiciário.

3 REFERÊNCIAS E FUNDAMENTAÇÃO LEGAL

3.1 Norma Técnica ABNT NBR ISO/IEC 27001:2022, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da Organização.

3.2 Norma Técnica ABNT NBR ISO/IEC 27002:2022, que fornece diretrizes para práticas de gestão de segurança da informação.

3.3 Portaria n. 162/2021-CNJ, que aprova Protocolos e Manuais criados pela Resolução n. 396/2021-CNJ, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

3.4 Lei Geral de Proteção de Dados (LGPD) - Lei n. 13.709/2018, que estabelece regras para o tratamento de dados pessoais, garantindo a privacidade e a proteção das informações, especialmente relevantes no contexto judiciário.

3.5 Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011, que regulamenta o acesso a informações públicas, reforçando a importância da segurança na gestão e divulgação dessas informações.

4 GLOSSÁRIO

4.1 ***Proxy/web-proxy*** - também conhecido por filtro de conteúdo, é o servidor responsável por intermediar o acesso à internet, aplicando regras de controle de acesso e mecanismos de proteção contra códigos maliciosos, previamente configurados, e por controlar a alocação de recursos de rede.

4.2 ***Proxy/web-proxy*** **Externo** - são servidores não gerenciados pelo PJRO, responsáveis por intermediar o acesso à internet, que não aplicam as regras de controle de acesso e mecanismos de proteção da mesma forma que o proxy do PJRO.

4.3 **Sítio** - é um conjunto de páginas web organizadas a partir de um URL básico, onde fica a página principal, e geralmente são armazenadas numa única pasta ou subpastas relacionadas no mesmo diretório de um servidor.

4.4 ***Malware*** - software malicioso projetado para infiltrar um sistema computacional com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela

empresa, como correio eletrônico ou sites. Entre os exemplos de malware estão os vírus, *worms, trojans* (ou cavalos de Troia), *spyware, adware e rootkits.*

4.5 ***Spam* -** mensagem eletrônica não solicitada enviada em massa.

4.6 **Ativos de TIC -** é o conjunto dos ativos de informação, ativos de rede, processos, funcionalidades e recursos de software e serviços de TIC.

4.7 **Confidencialidade -** princípio que a informação esteja indisponível ou não revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada.

4.8 **Integridade -** princípio que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

4.9 **Disponibilidade -** princípio que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

4.10 **Autenticidade -** propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

4.11 ***Decrypt* (descriptografar) -** a inspeção Decrypt tem o propósito de analisar o tráfego criptografado, assegurando a integridade e confidencialidade das informações, além de identificar possíveis atividades maliciosas que possam comprometer a segurança dos ativos de TIC do PJRO.

4.12 **NSIC -** Norma de Segurança da Informação Cibernética.

5 CONTROLES

5.1 O acesso à internet através das redes corporativas do PJRO será concedido exclusivamente a usuários autorizados e configurado pela Secretaria de Tecnologia da Informação e Comunicações.

5.2 A autorização mencionada no item 5.1 segue as diretrizes estabelecidas pela NSIC 01 - Gestão de Identidade e Controle de Acesso aos Recursos de TIC.

5.3 O tráfego de internet, tanto de entrada quanto de saída, será automaticamente inspecionado, monitorado, controlado e auditado pela ferramenta de proxy (filtro de conteúdo).

5.3.1 A ferramenta de proxy será configurada de acordo com os limites estabelecidos por esta norma ou definidos pelo CGSI - Comitê Gestor Multidisciplinar de Segurança da Informação e Cibernética.

5.3.2 Em caso de identificação de comportamentos suspeitos ou acessos não autorizados, medidas de resposta imediata e protocolos de segurança serão implementados.

5.4 Fica expressamente proibido o uso de métodos para contornar as políticas de bloqueio automaticamente implementadas no proxy do PJRO, como: uso de web-proxies externos, assim como túneis criptografados, entre outras práticas.

5.5 Os tráfegos relacionados aos ativos de TIC, como servidores, switches, aplicações web, entre outros, devem ter seus acessos de entrada e saída criptografados (SSL, SSH e outros) e submetidos à inspeção por meio de Decrypt.

5.6 A instalação do certificado digital, responsável pela criptografia e descriptografia do tráfego, deve ser realizada pelo profissional responsável pela gestão de cada ativo de TIC.

5.7 Os Ativos de TIC devem ter acesso restrito à internet, seguindo a regra padrão de bloqueio total, com liberação apenas do estritamente necessário.

5.7.1 O responsável pelo ativo deve informar, de maneira clara, a porta, o protocolo, a aplicação e o destino de saída/entrada necessários para a comunicação interna ou externa (Internet) do ativo.

5.8 O acesso à Internet será concedido aos usuários, desde que esteja relacionado às atribuições do cargo ou função, observando as seguintes condições:

5.8.1 Não ser abusivo;

5.8.2 Não representar risco à segurança cibernética;

5.8.3 Não comprometer o desempenho da rede; e

5.8.4 Observância aos deveres e vedações do Código de Ética e Conduta do Poder Judiciário do Estado de Rondônia.

5.9 É vedado a todo(a) agente do Poder Judiciário do Estado de Rondônia, sem prejuízo das demais obrigações legais e regulamentares, a divulgação ou facilitação à divulgação de informações sigilosas obtidas em razão do cargo ou função e, ainda, de relatórios, instruções e informações de processos cujos objetos ainda não tenham sido apreciados, sem prévia autorização da autoridade competente.

5.10 É vedado aos usuários de TIC:

5.10.1 Compartilhar software produzido ou licenciado ao PJRO sem a prévia autorização do Presidente do TJRO.

5.10.2 Utilizar os recursos do PJRO com o intuito deliberado de propagar qualquer tipo de Malware (vírus, *worm*, cavalo de troia, *spam*), bem como praticar assédio, discriminação, discurso de ódio ou perturbação.

5.10.3 Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a política de segurança cibernética, como pornografia, pedofilia, racismo, jogos, páginas de distribuição e compartilhamento de arquivos que violem a propriedade intelectual e que não tenham relação com o trabalho exercido na unidade.

5.10.4 Utilizar programas e/ou acessar páginas de troca de mensagens em tempo real (bate-papo), armazenamento online, áudio ou vídeo em tempo real ou sob demanda, exceto os fornecidos e/ou autorizados por este tribunal;

5.10.5 Acessar sítios que representem ameaça à segurança cibernética ou que possam comprometer de alguma forma a integridade da rede do PJRO;

5.10.6 Acessar ou fazer upload/download de arquivos não relacionados ao trabalho, especialmente músicas, imagens, vídeos, jogos e programas de qualquer tipo.

5.11 Cabe ao gestor da unidade orientar os usuários sob sua subordinação sobre o uso adequado dos recursos de internet, conforme as regras estabelecidas neste normativo, além de reportar à GPTIR qualquer descumprimento destas diretrizes.

5.12 Serão adotadas medidas para assegurar a manutenção da disponibilidade e qualidade do acesso à internet, tanto em situações normais de funcionamento quanto em contingências, a critério da Secretaria de Tecnologia da Informação e Comunicação - STIC.

5.12.1 As medidas podem incluir bloqueios totais ou parciais, priorização de acessos a determinados sítios e serviços, e limitação da banda de tráfego de dados.

5.13 As medidas adotadas no item anterior serão comunicadas aos usuários afetados de acordo com a natureza da medida implementada.

5.14 A STIC poderá, a qualquer momento, implementar filtros de conteúdo na web para bloquear o acesso a sites maliciosos, potencialmente perigosos ou não relacionados ao trabalho.

5.15 A STIC poderá exigir aprovação prévia para downloads, reduzindo o risco de instalação de aplicativos não autorizados.

6 MONITORAMENTO E AUDITORIA

6.1 Por razões de segurança, todo acesso à Internet será monitorado, e os registros de acessos e seus responsáveis serão mantidos pela Secretaria de Tecnologia da Informação e Comunicação por um período mínimo de 6 (seis) meses, podendo se estender até 12 (doze) meses.

6.2 Em caso de indícios de descumprimento das diretrizes deste normativo, o Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética (GPTIR) poderá, por iniciativa própria ou por determinação do Comitê Gestor de Segurança da Informação e Cibernética, realizar auditoria sobre os fatos. Salienta-se a importância da colaboração ativa dos usuários durante esse processo, fornecendo informações necessárias para uma análise completa e eficaz.

6.3 Os relatórios das auditorias ordinárias e extraordinárias realizadas pelo GPTIR serão encaminhados ao Comitê Gestor de Segurança da Informação para análise e deliberação, para aprimorar as práticas de segurança, identificar áreas de melhoria e garantir a eficácia contínua das medidas adotadas.

7 DISPOSIÇÃO FINAL

7.1 O disposto na presente norma será atualizado sempre que alterados os procedimentos e controles ou quando necessário, mediante iniciativa do CGSI.

ANEXO V

RESOLUÇÃO N. 350/2025-TJRO

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

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA (PSIC)

NORMA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA

NSIC 03 - REDE WI-FI

PRESIDENTE
Desembargador Raduan Miguel Filho

VICE-PRESIDENTE
Desembargador Glodner Luiz Pauletto

CORREGEDOR-GERAL
Desembargador Gilberto Barbosa Batista dos Santos

SECRETÁRIO GERAL
Juiz Rinaldo Forti Silva

SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Ângela Carmen Szymczak de Carvalho

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO MULTIDISCIPLINAR
Desembargador Glodner Luiz Pauletto
Desembargador Gilberto Barbosa Batista dos Santos
Juíza Valdirene Alves da Fonseca Clementele
Elaine Piacentini Bettanin
Jucélio Scheffmacher de Souza
Ângela Carmen Szymczak de Carvalho
Rosemeire Moreira Ferreira
Fabiano Sergio Paiva Dias de Sá
Gustavo Luiz Sevagnan Nicocelli
Eduardo Luiz Will Bezerra
Reginaldo de Souza Gadelha
Ignácio de Loiola Reis Junior
Hilton José de Santana Pinto

COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Ângela Carmen Szymczak de Carvalho

Alessandra Lima Costa
Reginaldo de Souza Gadelha
Simone Soares Sena de Oliveira

EQUIPE DE ELABORAÇÃO

Allan Tito Leite Ratts
Ângela Carmen Szymczak de Carvalho
Fernanda Soares Lana
Ignacio de Loiola Reis Junior
Jorge Willians da Silva Ferreira Batista
Reginaldo de Souza Gadelha
Sidnei Roberto Feliciano da Silva
Simone Soares Sena de Oliveira
Tárik Kamel de Oliveira
Thiago Fleury Marques Cotrim

REGISTRO DE REVISÕES

Política de Segurança da Informação (PSI)				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	novembro/2014	Criação da política.	Sesinf	Coinf
2	janeiro/2017	Acréscimo de critérios para acessar o datacenter principal. Formalizada por meio da Resolução n. 036/2016, republicada em 2017 por erro material.	DISEIN DIESE	Tribunal Pleno
3	abril/2019	Atualização da Política. Formalizada por meio da Resolução n. 088/2019.	DISEIN DIESE	CGSI

4	novembro/2020	Alteração na gestão do serviço de correio eletrônico institucional. Formalizada por meio do Ato n. 1.111/2020.	DESEIN DISEIN DIESE	CGSI
5	junho/2021	Atualização sobre a atuação do Comitê Permanente de Segurança do Poder Judiciário. Formalizada por meio da Resolução n. 209/2021.	DESEIN DISEIN DIESE	CGSI

Política da Segurança da Informação Cibernética (PSIC) NSIC 03 - Rede Wi-FI				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	junho/2025	Alteração na Resolução para focar na segurança da informação cibernética e criação de anexos específicos para tratar cada tema individualmente.	DESEIN DISEIN DIESE	Cgestic CGSI

1 OBJETIVO

1.1 O objetivo primordial desta norma é estabelecer diretrizes, padrões e práticas de segurança da informação para a rede Wi-Fi do PJRO - Poder Judiciário do Estado de Rondônia. O intuito é garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas vinculados à rede, mitigando riscos e protegendo as informações sensíveis sob a responsabilidade do PJRO.

1.2 A norma visa promover um ambiente seguro e confiável, através da implementação de controles adequados, visando à prevenção de acessos não autorizados, ataques cibernéticos e outras ameaças que possam comprometer a segurança da rede Wi-Fi. Além disso, busca-se assegurar a conformidade com regulamentações pertinentes à proteção de dados e à segurança da informação, fortalecendo a postura do PJRO diante de desafios emergentes no cenário digital.

2 MOTIVAÇÃO

2.1 A crescente digitalização e interconexão de sistemas e dados no ambiente judicial demandam uma atenção especial à segurança da informação. A rede Wi-Fi do PJRO desempenha um papel crucial na transmissão e acesso a informações sensíveis, exigindo

medidas robustas para salvaguardar a integridade, confidencialidade e disponibilidade desses dados.

2.2 A motivação por trás desta norma é abordar os desafios emergentes relacionados à cibersegurança e proteção de dados no contexto do PJRO. Aumentar a segurança da rede Wi-Fi é essencial para proteger as comunicações, dados judiciais e informações confidenciais contra ameaças cibernéticas, garantindo a continuidade dos serviços judiciais.

2.3 A implementação desta norma busca também atender às regulamentações vigentes relacionadas à segurança da informação, fornecendo um arcabouço sólido para a conformidade legal. Além disso, a norma visa fortalecer a confiança do público, advogados, magistrados e demais partes envolvidas no sistema judicial, demonstrando o comprometimento do PJRO com a proteção diligente e responsável das informações sob sua responsabilidade.

2.4 A norma reflete a compreensão da importância estratégica da segurança da informação como parte integrante da governança judiciária, promovendo uma cultura de segurança proativa e contínua. Ao adotar essa abordagem, o PJRO busca assegurar a confiança nas operações judiciais, protegendo os interesses legais e garantindo a justiça por meio da preservação segura e eficaz da informação na rede Wi-Fi.

2.5 Disciplinar por meio da conscientização e controles o uso aceitável e seguro da Rede Wi-Fi.

3 REFERÊNCIAS E FUNDAMENTAÇÃO LEGAL

3.1 Norma Técnica ABNT NBR ISO/IEC 27001:2022, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da Organização.

3.2 Norma Técnica ABNT NBR ISO/IEC 27002:2022, que fornece diretrizes para práticas de gestão de segurança da informação.

3.3 Portaria n. 162/2021-CNJ, que aprova Protocolos e Manuais criados pela Resolução n. 396/2021-CNJ, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

3.4 Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018, que estabelece regras para o tratamento de dados pessoais, garantindo a privacidade e a proteção das informações, especialmente relevantes no contexto judiciário.

3.5 Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011, que regulamenta o acesso a informações públicas, reforçando a importância da segurança na gestão e divulgação dessas informações.

4 GLOSSÁRIO

4.1 **Rede Wi-Fi do PJRO:** infraestrutura de comunicação sem fio utilizada pelo PJRO para a transmissão de dados, acesso à Internet e comunicação entre dispositivos dentro de suas instalações.

4.2 **SSID (Service Set Identifier):** identificador único atribuído à rede Wi-Fi, ou seja, é o "nome" da rede Wi-Fi, que permite que dispositivos a reconheçam e se conectem a ela. Como por exemplo, a rede "PJRO-MOVEL" utilizada no edifício sede. A norma define práticas seguras para a configuração e gestão do SSID.

4.3 **Dispositivo móvel:** qualquer equipamento portátil, como notebooks, tablets, **s**martphones, handhelds e semelhantes;

4.4 **Dispositivo institucional:** qualquer dispositivo registrado como patrimônio do PJRO;

4.5 **Dispositivo particular:** qualquer dispositivo não registrado como patrimônio do PJRO.

4.6 **Rede corporativa:** conjunto de redes do PJRO para uso em dispositivos institucionais e/ou particulares destinado a servidores(as), estagiários(as), funcionários(as) terceirizados(as) contratados(as) e magistrados(as) do PJRO.

4.7 **Confidencialidade**: princípio que a informação esteja indisponível ou não revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada.

4.8 **Integridade**: princípio que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

4.9 **Disponibilidade**: princípio que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

4.10 **Autenticidade**: propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

4.11 **Autenticação:** Processo pelo qual os dispositivos e usuários são verificados antes de serem autorizados a acessar a rede Wi-Fi. Inclui métodos de autenticação robustos, como WPA2 ou WPA3, para garantir a segurança.

4.12 **Criptografia:** Técnica utilizada para proteger a confidencialidade dos dados transmitidos pela rede Wi-Fi. A norma define o uso obrigatório de protocolos de criptografia fortes para proteger as comunicações.

4.13 **Política de Senhas:** Estabelece requisitos para a criação, gerenciamento e proteção de senhas utilizadas para autenticação na rede Wi-Fi, promovendo a segurança contra acessos não autorizados.

4.14 **Monitoramento de Tráfego:** Práticas para o acompanhamento contínuo do tráfego na rede Wi-Fi, identificando padrões suspeitos, comportamentos anômalos e potenciais ameaças à segurança da informação.

4.15 **Gestão de Incidentes:** Define procedimentos para identificação, notificação, contenção e resposta a incidentes de segurança na rede Wi-Fi, visando minimizar danos e garantir a rápida recuperação.

4.16 **Conscientização e Treinamento:** Estratégias para promover a conscientização entre os usuários da rede Wi-Fi do PJRO, incluindo treinamentos regulares sobre práticas seguras, ameaças cibernéticas e procedimentos de segurança.

4.17 **Atualizações e Manutenção:** Diretrizes para a aplicação regular de atualizações de segurança em dispositivos de rede, sistemas operacionais e softwares relacionados à infraestrutura Wi-Fi.

4.18 **Responsabilidades e Conformidade:** Estabelece as responsabilidades individuais e organizacionais relacionadas à segurança da informação na rede Wi-Fi, garantindo a conformidade com as políticas estabelecidas.

4.19 **Dados Sensíveis:** Informações que, se comprometidas, podem causar danos significativos ao PJRO, a partes envolvidas ou indivíduos associados. Isso inclui dados judiciais, informações pessoais e outros dados confidenciais.

4.20 **WPA2 (*Wi-Fi Protected Access* 2)**: protocolo de segurança criptografado que protege o tráfego da internet em redes sem fio.

4.21 **WPA3 (*Wi-Fi Protected Access* 3)**: protocolo de segurança criptografado que protege o tráfego da internet em redes sem fio sendo, uma evolução do protocolo WPA2.

4.22 **Wi-Fi:** tecnologia de conexão sem fio que conecta dispositivos a uma rede.

4.23 ***Firmware***: é um tipo de software essencial que reside em um dispositivo eletrônico e controla suas funções básicas. Ele atua como um intérprete entre o sistema operacional do dispositivo e seus componentes de hardware, fornecendo instruções detalhadas sobre como operar cada componente.

4.24 ***Firewall***: sistema de segurança que atua como uma barreira de segurança entre a rede e o mundo online, protegendo os dispositivos e dados contra acessos não autorizados e outras ameaças cibernéticas.

4.25 **WPS (Wi-Fi Protected Setup):** padrão de segurança aplicado à configuração de Wi-Fi.

4.26 **NSIC**: Norma de Segurança da Informação Cibernética.

5 CONTROLES

5.1 As redes Wi-Fi Corporativas são definidas através de SSIDs com as seguintes nomenclaturas:

5.1.1 **PJRO:** Rede destinada aos servidores e magistrados do PJRO na capital e no interior, é uma extensão da rede cabeada (rede corporativa), disponível para utilização nos dispositivos institucionais.

5.1.2 **PJRO IoT:** Rede destinada aos dispositivos institucionais que requerem autenticação especial.

5.1.3 **PJRO Móvel:** Rede destinada aos dispositivos particulares dos servidores e magistrados do PJRO, sem acesso à rede corporativa do PJRO, para ter acesso à internet utilizando o mesmo usuário e senha da rede corporativa.

5.1.4 **PJRO Visitante:** Rede com tempo de acesso predefinido, destinada aos jurisdicionados, permitindo o acesso à internet sem acesso à rede corporativa do PJRO.

5.1.5 **MPRO:** Rede destinada a atender ao convênio entre Ministério Público e Tribunal de Justiça, sem acesso à rede corporativa do PJRO, mas com acesso à rede corporativa do MPRO e a internet para atender as necessidades dos membros do MPRO.

5.2 A criação de outras SSIDs ou a remoção de SSIDs existentes dependerá da aprovação do CGSI.

5.3 O acesso à rede sem fio estará disponível 24h (vinte e quatro horas) por dia.

5.3.1 O SSID "**PJRO Visitante**" terá os seguintes controles:

5.3.1.1 Para acessar, o visitante deve fazer o cadastro pessoalmente na recepção das unidades do PJRO, pois é vedada a utilização anônima da rede.

5.3.1.2 O cadastro citado no item 5.3.1.1 requer a apresentação de um documento de identificação pessoal oficial com foto, número de telefone, correio eletrônico válido para receber as credenciais e o CPF para realizar o login.

5.3.1.3 A credencial de acesso a essa rede terá prazo de validade de 24h (vinte e quatro horas).

5.3.1.3.1 A credencial dos alunos e professores da Emeron, advogados, procuradores, defensores públicos e magistrados visitantes terão prazo de validade de 90 (noventa) dias, não se aplicando assim, o prazo de 24h (vinte e quatro horas) mencionado no item 5.3.1.3.

5.3.1.3.2 Em caso de eventos realizados pelo PJRO, poderá ser realizado um pré-cadastro ou validade personalizada, de acordo com o tempo de participação do evento.

5.3.1.4 A credencial poderá ser usada no máximo em até 2 (dois) dispositivos simultaneamente.

5.4 Cabe à STIC orientar os servidores e magistrados sobre o uso adequado da rede Wi-Fi.

5.4.1 A STIC não prestará suporte técnico, manutenção, configuração, instalação e desinstalação de softwares em dispositivos particulares.

5.4.2 A STIC poderá orientar os usuários que não consigam conectar seu dispositivo móvel às redes Wi-Fi do PJRO.

5.5 Todos os dispositivos móveis ou sistemas que se conectem à rede Wi-Fi do PJRO estão sujeitos às mesmas políticas, procedimentos e práticas que regulam o uso e o funcionamento de qualquer dispositivo ou sistema conectado à rede corporativa do PJRO.

5.6 O uso da internet está vinculado à conta do usuário e seu respectivo dispositivo de acesso à rede Wi-Fi. Caso constem acessos indevidos, ou inapropriados, os usuários serão notificados e poderão ter seu acesso e dispositivo bloqueados sendo responsabilizado por qualquer dano causado às redes do PJRO.

5.7 As redes Wi-Fi devem aplicar criptografia robusta para proteger a confidencialidade das informações transmitidas pela rede.

5.8 A autenticação nas redes Wi-Fi do PJRO deverá seguir as diretrizes da norma de Gestão de Identidade e Controle de Acesso.

5.9 A STIC deve:

5.9.1 Desativar a transmissão do SSID da rede Wi-Fi **"PJRO IoT"** para reduzir a visibilidade da rede, tornando mais difícil para invasores identificarem e se conectarem à rede.

5.9.2 Implementar ferramentas de monitoramento para identificar padrões suspeitos ou atividades anômalas na rede. Isso inclui a detecção de dispositivos não autorizados.

5.9.3 Manter regularmente atualizados os *firmwares* de dispositivos de rede, como roteadores e pontos de acesso, e garantir que todos os softwares relacionados à segurança estejam na versão mais recente.

5.9.4 Configurar firewalls para controlar o tráfego de entrada e saída na rede Wi-Fi, restringindo o acesso não autorizado e bloqueando atividades maliciosas.

5.9.5 Implementar medidas para isolar dispositivos na rede "**PJRO Visitante**" e "**PJRO Móvel**", limitando a comunicação entre eles. Isso ajuda a conter possíveis ameaças caso um dispositivo seja comprometido.

5.9.6 Manter um inventário atualizado de todos os dispositivos conectados à rede Wi-Fi, facilitando a identificação rápida de dispositivos não autorizados ou suspeitos.

5.9.7 Configurar a rede para desconectar automaticamente dispositivos inativos por um determinado período de tempo, reduzindo o risco de acesso não autorizado em caso de dispositivos perdidos, furtados, roubados etc.

5.9.8 Dividir a rede em segmentos para limitar o acesso de dispositivos a determinadas partes da infraestrutura, reduzindo assim a superfície de ataque em caso de comprometimento.

5.9.9 Configurar a potência do sinal Wi-Fi de forma a limitar sua abrangência ao ambiente necessário, minimizando a exposição da rede a possíveis ataques externos.

5.9.10 Implementar uma política abrangente de logs para registrar eventos relevantes na rede Wi-Fi. A análise desses logs pode auxiliar na detecção precoce de atividades suspeitas.

5.9.11 Realizar auditorias regulares de segurança na rede Wi-Fi para identificar possíveis vulnerabilidades e garantir a conformidade contínua com as políticas estabelecidas.

5.9.12 Implementar medidas de proteção contra ataques de força bruta, como bloqueio temporário, conforme item 5.21.1 da "NSIC 01 - Gestão de Identidade e Controle de Acesso" desta Política.

5.9.13 Desativar o *WPS*, se não for essencial, para evitar possíveis vulnerabilidades associadas a esse recurso.

5.9.14 Utilizar listas de controle de acesso (ACLs) para gerenciar quais dispositivos específicos têm permissão para se conectar à rede Wi-Fi.

5.9.15 Realizar backups regulares das configurações da rede Wi-Fi para facilitar a recuperação em caso de falhas ou incidentes.

5.9.16 Promover programas regulares de treinamento e conscientização em segurança da informação para usuários da rede Wi-Fi, destacando boas práticas e alertando sobre ameaças em evolução.

6 MONITORAMENTO E AUDITORIA

6.1 Por motivos de segurança, todo acesso à Rede Wi-Fi será monitorado, e os registros serão mantidos pela Secretaria de Tecnologia da Informação e Comunicação por no mínimo 6 (seis) meses e até 12 (doze) meses.

6.2 Em caso de indícios de descumprimento das diretrizes previstas neste normativo, o Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética poderá de ofício ou por determinação do Comitê Gestor de Segurança da Informação e Cibernética realizar auditoria sobre os fatos.

6.3 Os relatórios decorrentes das auditorias ordinárias e extraordinárias realizadas pelo Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética serão encaminhados ao Comitê Gestor de Segurança da Informação, para análise e deliberação.

7 DISPOSIÇÃO FINAL

7.1 O disposto na presente norma será atualizado sempre que alterados os procedimentos e controles ou quando necessário, mediante iniciativa do CGSI.

ANEXO VI

RESOLUÇÃO N. 350/2025-TJRO

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

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA (PSIC)

NORMA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA

NSIC 04 - ACESSO REMOTO E USO DA VPN

PRESIDENTE
Desembargador Raduan Miguel Filho

VICE-PRESIDENTE
Desembargador Glodner Luiz Pauletto

CORREGEDOR-GERAL
Desembargador Gilberto Barbosa Batista dos Santos

SECRETÁRIO GERAL

Juiz Rinaldo Forti Silva

SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO MULTIDISCIPLINAR

Desembargador Glodner Luiz Pauletto

Desembargador Gilberto Barbosa Batista dos Santos

Juíza Valdirene Alves da Fonseca Clementele

Elaine Piacentini Bettanin

Jucélio Scheffmacher de Souza

Ângela Carmen Szymczak de Carvalho

Rosemeire Moreira Ferreira

Fabiano Sergio Paiva Dias de Sá

Gustavo Luiz Sevagnan Nicocelli

Eduardo Luiz Will Bezerra

Reginaldo de Souza Gadelha

Ignácio de Loiola Reis Junior

Hilton José de Santana Pinto

COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

Alessandra Lima Costa

Reginaldo de Souza Gadelha

Simone Soares Sena de Oliveira

EQUIPE DE ELABORAÇÃO

Allan Tito Leite Ratts

Ângela Carmen Szymczak de Carvalho

Fernanda Soares Lana

Ignacio de Loiola Reis Junior
Jorge Willians da Silva Ferreira Batista
Reginaldo de Souza Gadelha
Sidnei Roberto Feliciano da Silva
Simone Soares Sena de Oliveira
Tárik Kamel de Oliveira
Thiago Fleury Marques Cotrim

REGISTRO DE REVISÕES

Política de Segurança da Informação (PSI)				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	novembro/2014	Criação da política.	Sesinf	Coinf
2	janeiro/2017	Acréscimo de critérios para acessar o datacenter principal. Formalizada por meio da Resolução n. 036/2016, republicada em 2017 por erro material.	DISEIN DIESE	Tribunal Pleno
3	abril/2019	Atualização da Política. Formalizada por meio da Resolução n. 088/2019.	DISEIN DIESE	CGSI
4	novembro/2020	Alteração na gestão do serviço de correio eletrônico institucional. Formalizada por meio do Ato n. 1.111/2020.	DESEIN DISEIN DIESE	CGSI
5	junho/2021	Atualização sobre a atuação do Comitê Permanente de Segurança do Poder Judiciário. Formalizada por meio da Resolução n. 209/2021.	DESEIN DISEIN DIESE	CGSI
Política da Segurança da Informação Cibernética (PSIC) **NSIC 04 - Acesso Remoto e Uso da VPN**				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	junho/2025	Alteração na Resolução para focar na segurança da informação cibernética e criação de anexos específicos para tratar cada tema individualmente.	DESEIN DISEIN DIESE	Cgestic CGSI

1 OBJETIVO

1.1 Estabelecer diretrizes, padrões e boas práticas para acesso remoto à rede corporativa do Poder Judiciário do Estado de Rondônia.

2 MOTIVAÇÃO

2.1 Disciplinar, por meio da conscientização e controles, o acesso remoto à rede corporativa do PJRO;

2.2 Proteção da Confidencialidade, Integridade, Disponibilidade e Autenticidade das Informações do PJRO;

2.3 Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

3 REFERÊNCIAS E FUNDAMENTAÇÃO LEGAL

3.1 Norma Técnica ABNT NBR ISO/IEC 27001:2022, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.2 Norma Técnica ABNT NBR ISO/IEC 27002:2022, que fornece diretrizes para práticas de gestão de segurança da informação.

3.3 Portaria nº 162/2021-CNJ, que aprova protocolos e manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

3.4 Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018, que estabelece regras para o tratamento de dados pessoais, garantindo a privacidade e a proteção das informações, especialmente relevantes no contexto judiciário.

3.5 Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011, que regulamenta o acesso a informações públicas, reforçando a importância da segurança na gestão e divulgação dessas informações.

4 GLOSSÁRIO

4.1 Acesso Remoto: toda conexão estabelecida à rede do PJRO originada de um ponto externo.

4.2 Acesso via VPN: Toda conexão estabelecida por servidores, magistrados ou terceirizados à rede corporativa do PJRO originada de um ponto externo, utilizando cadastro do AD (Active Directory), para acessar serviços de TIC disponibilizados internamente na rede corporativa do PJRO (sem acesso externo).

4.3 Chefia imediata: magistrado, comissionado ou servidor ocupante de cargo em comissão ou função comissionada, ao qual o servidor está diretamente subordinado.

4.4 Risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização.

4.5 Gestão de Vulnerabilidades de TIC: processo de gestão que visa conhecer, monitorar e tratar vulnerabilidades que afetem os ativos de TIC, minimizando o risco de que as mesmas sejam exploradas.

4.6 Ativo de informação: todo dado ou informação gerado, adquirido, utilizado ou custodiado pelo PJRO, assim como qualquer equipamento, software ou recurso utilizado para seu processamento ou armazenamento.

4.7 Serviço de TIC: serviço baseado no uso da Tecnologia da Informação e Comunicação, provido a um ou mais clientes para apoiar os processos de negócio da instituição.

4.8 Ativo de TIC: é o conjunto dos ativos de informação, ativos de rede, processos, funcionalidades e recursos de software e serviços de TIC.

4.9 Confidencialidade: princípio que a informação esteja indisponível ou não revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada.

4.10 Integridade: princípio que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

4.11 Disponibilidade: princípio que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

4.12 Autenticidade: propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

4.13 VPN (Virtual Private Network): rede privada virtual que visa criar uma conexão segura e criptografada.

4.14 Crack (Craquear): ato de quebrar um sistema por meio de um programa para utilização de recursos que dependem de licenciamento.

5 CONTROLES

Seção I - Requisitos Mínimos de segurança

5.1 Os equipamentos utilizados para acessar os serviços de acesso remoto e acesso via VPN do PJRO, deverão ter os requisitos mínimos de segurança:

5.1.1 Tenha um sistema operacional seguro com as seguintes características:

5.1.1.1 Que não seja falsificado, crackeado ou desbloqueado (jailbreak);

5.1.1.2 Que esteja na lista de homologados pelo Tribunal de Justiça do Estado de Rondônia; e

5.1.1.3 Que esteja com as últimas atualizações de segurança fornecidas pelo fabricante.

5.1.2 Tenha um software de antivírus:

5.1.2.1 Que seja original, isto é, que não seja falsificado ou crackeado.

5.1.2.2 Que esteja na lista de homologados pelo Tribunal de Justiça do Estado de Rondônia.

5.1.2.3 Que esteja habilitado e com as últimas atualizações de segurança fornecidas pelo fabricante.

5.1.3 Tenha uma solução de firewall particular:

5.1.3.1 Que o sistema de firewall pessoal esteja devidamente habilitado, seja ele do próprio sistema operacional ou integrado à solução de antivírus.

5.2 Os equipamentos que não estiverem em conformidade com os requisitos mínimos de segurança definidos pela STIC, não poderão utilizar o acesso remoto e o acesso via VPN para se conectar aos Ativos de TIC do PJRO.

Seção II - Acesso a VPN

5.3. O acesso via VPN (Redes Privadas Virtuais) à rede corporativa do PJRO deverá ser realizado de modo seguro, por meio de criptografia, múltiplo fator de autenticação (MFA - *Multi Factor Authentication)*.

5.4 O acesso via VPN deve ser concedido por um período de tempo pré-definido com base no pedido realizado pela chefia imediata.

5.4.1 O pedido de acesso via VPN para os usuários deve ser realizado através da Central de Serviços, com justificativa, serviço e/ou rede e período a serem utilizados.

5.4.2 Após a abertura do chamado, o mesmo deverá ser direcionado para aprovação do Gestor do Ativo de TIC.

5.4.3 Em situações específicas, analisado o aspecto de segurança, a STIC poderá encerrar ou alterar o período de acesso via VPN.

5.5 Os sistemas de uso internos do PJRO, que são utilizados exclusivamente por magistrados e servidores, quando acessados de fora da rede corporativa do PJRO, deverão ser obrigatoriamente acessados através da VPN.

5.6 É permitido o uso de VPN para os seguintes serviços:

5.6.1 HTTP e HTTPS - Sistemas Internos do PJRO;

5.6.2 Sistemas específicos poderão ter os serviços liberados, quando estritamente necessário, desde que:

5.6.2.1 Seja devidamente justificado pelo gestor da unidade;

5.6.2.2 Tenha a anuência do gestor do ativo de TIC a ser acessado;

5.6.2.3 Mediante autorização do CGSI;

5.6.2.4 Caso seja autorizado, os aplicativos serão instalados na máquina pessoal do servidor ou magistrado;

5.7 Não é permitido o uso de VPN para os seguintes serviços:

5.7.1 Protocolo RDP - Acesso remoto a estação de trabalho;

5.7.2 Os Protocolos SMB, NFS, pastas compartilhadas, e outros serviços com as mesmas características;

5.7.3 Em casos excepcionais, outros serviços poderão ser liberados para as equipes responsáveis pela infraestrutura e segurança de TIC do PJRO, mediante autorização do(a) Secretário(a) de TIC.

Seção III - Acesso Remoto

5.8. O acesso remoto aos ativos de TIC do PJRO será permitido em caráter excepcional e somente para fins de trabalho.

5.9 Empresas que possuem vínculo contratual com o PJRO para prestação de serviços de suporte técnico a sistemas e infraestrutura de Tecnologia da Informação poderão realizar acessos remotos aos ativos de TIC a fim de efetuar as configurações necessárias na resolução de demandas técnicas.

5.9.1 Enquanto durar o acesso remoto, o responsável pelo ativo de TIC deverá acompanhar todos os procedimentos efetuados pela empresa prestadora de serviço de suporte técnico.

5.10 O acesso remoto deve ser concedido por um período de tempo pré-definido com base no pedido realizado pela chefia imediata.

5.10.1 O pedido de acesso remoto para os usuários deve ser realizado através da Central de Serviços, com justificativa, serviço e/ou rede e período a serem utilizados.

5.10.2 Após a abertura do chamado, o mesmo deverá ser direcionado para aprovação do Gestor do Ativo de TIC.

5.10.3 Em situações específicas, analisado o aspecto de segurança, a STIC poderá encerrar ou alterar o período de acesso remoto.

5.11 O acesso remoto somente será permitido por meio de soluções homologadas pelo PJRO.

5.11.1 Os acessos aos ativos de infraestrutura de TIC utilizarão por padrão serviço que conceda acesso seguro e temporário aos dispositivos da rede corporativa.

5.11.2 Caso não seja possível acessar por meio de soluções já homologadas, o usuário deverá solicitar a análise de outra solução, conforme Processo de Homologação de Software de Terceiro.

5.12 O acesso remoto poderá ser interrompido a qualquer momento, independentemente de comunicação ao(a) usuário(a), na hipótese de ser identificada situação de ameaça ou risco à integridade da rede corporativa e aos serviços disponíveis do PJRO.

5.13 O(a) usuário(a) que tomar conhecimento ou suspeitar de quaisquer falhas ou indícios de vulnerabilidade de segurança da informação deve comunicar, imediatamente, o fato à STIC.

6 MONITORAMENTO E AUDITORIA

6.1 Por motivos de segurança, todo acesso remoto será monitorado, e os registros serão mantidos pela Secretaria de Tecnologia da Informação e Comunicação por no mínimo 6 (seis) meses e até 12 (doze) meses.

6.2 Em caso de indícios de descumprimento das diretrizes previstas neste normativo, o Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética poderá de ofício ou por determinação do Comitê Gestor de Segurança da Informação e Cibernética realizar auditoria sobre os fatos.

6.3 Os relatórios decorrentes das auditorias ordinárias e extraordinárias realizadas pelo Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética serão encaminhados ao Comitê Gestor de Segurança da Informação, para análise e deliberação.

7 DISPOSIÇÃO FINAL

7.1 O disposto na presente norma será atualizado sempre que alterados os procedimentos e controles ou quando necessário, mediante iniciativa do CGSI.

ANEXO VII

RESOLUÇÃO N. 350/2025-TJRO

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

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA (PSIC)

NORMA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA

NSIC 05 - CORREIO ELETRÔNICO INSTITUCIONAL

SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO MULTIDISCIPLINAR

Desembargador Glodner Luiz Pauletto

Desembargador Gilberto Barbosa Batista dos Santos

Juíza Valdirene Alves da Fonseca Clementele

Elaine Piacentini Bettanin

Jucélio Scheffmacher de Souza

Ângela Carmen Szymczak de Carvalho

Rosemeire Moreira Ferreira

Fabiano Sergio Paiva Dias de Sá

Gustavo Luiz Sevagnan Nicocelli

Eduardo Luiz Will Bezerra

Reginaldo de Souza Gadelha

Ignácio de Loiola Reis Junior

Hilton José de Santana Pinto

COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

Alessandra Lima Costa

Reginaldo de Souza Gadelha

Simone Soares Sena de Oliveira

EQUIPE DE ELABORAÇÃO

Allan Tito Leite Ratts

Ângela Carmen Szymczak de Carvalho

Fernanda Soares Lana

Ignacio de Loiola Reis Junior

Jorge Willians da Silva Ferreira Batista
Reginaldo de Souza Gadelha
Sidnei Roberto Feliciano da Silva
Simone Soares Sena de Oliveira
Tárik Kamel de Oliveira
Thiago Fleury Marques Cotrim

REGISTRO DE REVISÕES

Política de Segurança da Informação (PSI)				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	novembro/2014	Criação da política.	Sesinf	Coinf
2	janeiro/2017	Acréscimo de critérios para acessar o datacenter principal. Formalizada por meio da Resolução n. 036/2016, republicada em 2017 por erro material.	DISEIN DIESE	Tribunal Pleno
3	abril/2019	Atualização da Política. Formalizada por meio da Resolução n. 088/2019.	DISEIN DIESE	CGSI
4	novembro/2020	Alteração na gestão do serviço de correio eletrônico institucional. Formalizada por meio do Ato n. 1.111/2020.	DESEIN DISEIN DIESE	CGSI
5	junho/2021	Atualização sobre a atuação do Comitê Permanente de Segurança do Poder Judiciário. Formalizada por meio da Resolução n. 209/2021.	DESEIN DISEIN DIESE	CGSI
Política da Segurança da Informação Cibernética (PSIC) **NSIC 05 - Correio Eletrônico Institucional**				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**

1	junho/2025	Alteração na Resolução para focar na segurança da informação cibernética e criação de anexos específicos para tratar cada tema individualmente.	DESEIN DISEIN DIESE	Cgestic CGSI

1 OBJETIVO

Estabelecer diretrizes e padrões para o uso do Correio Eletrônico Institucional no âmbito do Poder Judiciário do Estado de Rondônia.

2 MOTIVAÇÃO

2.1 Disciplinar o uso seguro e ético do correio eletrônico no PJRO por meio da conscientização e controles.

2.2 Proteção da confidencialidade, integridade, disponibilidade e autenticidade das informações do PJRO.

2.3 Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

3 REFERÊNCIAS E FUNDAMENTAÇÃO LEGAL

3.1 Norma Técnica ABNT NBR ISO/IEC 27001:2022, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.2 Norma Técnica ABNT NBR ISO/IEC 27002:2022, que fornece diretrizes para práticas de gestão de segurança da informação.

3.3 Portaria n. 162/2021-CNJ, que aprova protocolos e manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

3.4 Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018, que estabelece regras para o tratamento de dados pessoais, garantindo a privacidade e a proteção das informações, especialmente relevantes no contexto judiciário.

3.5 Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011, que regulamenta o acesso a informações públicas, reforçando a importância da segurança na gestão e divulgação dessas informações.

4 GLOSSÁRIO

4.1 **Correio eletrônico institucional**: serviço eletrônico de comunicação que permite o envio e recebimento de mensagens entre usuários durante a execução das atividades institucionais, mantido pelo TJRO;

4.2 **Correio eletrônico externo**: qualquer serviço de correio eletrônico não disponibilizado pelo PJRO;

4.3 **Correio eletrônico pessoal:** conta de correio eletrônico externo de uso pessoal do servidor ou magistrado, que tenha registro nos sistemas do PJRO;

4.4 **Spam**: mensagem de correio eletrônico não solicitada, encaminhada para vários destinatários, contendo normalmente conteúdo promocional ou tentativas de fraude;

4.5 **Código malicioso**: termo genérico que se refere a todos os tipos de software que executam ações maliciosas, como vírus, *spywares*, etc.

4.6 **Caixa postal**: conta de correio eletrônico onde são armazenados os correios eletrônicos recebidos pelo usuário;

4.7 ***Phishing***: mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros.

4.8 **Conta desativada:** conta que foi impossibilitada, pela STIC, de fazer login.

4.9 **Conta inativa:** conta que não tem nenhuma atividade de login no correio eletrônico por um determinado período de tempo, sem ter sido desabilitada pela STIC.

4.10 **Confidencialidade**: princípio que a informação esteja indisponível ou não revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada.

4.11 **Integridade**: princípio que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

4.12 **Disponibilidade**: princípio que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

4.13 **Autenticidade**: propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

4.14 **NSIC**: Norma de Segurança da Informação Cibernética.

5 CONTROLES

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

5.2 O domínio oficial do serviço de correio eletrônico do PJRO é o **"@tjro.jus.br",** e da EMERON é o **"@emeron.edu.br**".

5.2.1 Não será permitida a criação de outros domínios para o serviço de correio eletrônico do PJRO.

5.2.2 As mensagens enviadas por outro domínio não serão consideradas mensagens oficiais.

Seção I - Da Caixa Postal Institucional Pessoal

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

5.4 É permitida a criação de conta de correio eletrônico corporativo para prestadores de serviço que realizem ações em nome do PJRO.

5.5 A Secretaria de Gestão de Pessoas (SGP) e o Departamento do Conselho da Magistratura (DECOM) deverão comunicar imediatamente à STIC, nos casos de falecimento, aposentadoria, cedência a outro órgão, retorno ao órgão de origem, desligamento, demissão ou exoneração de servidor.

5.5.1 Nos casos de cedência a outro órgão ou aposentadoria os magistrados/servidores deverão informar a SGP ou ao DECOM, o correio eletrônico pessoal, para ter acesso às informações do PJRO.

5.5.2 De posse da informação da SGP e/ou DECOM, incumbe à STIC:

5.5.2.1 Excluir a conta do correio eletrônico nos casos de falecimento, aposentadoria, retorno ao órgão de origem, desligamento, demissão ou exoneração, decorrido o prazo de 30 (trinta) dias, desde que realizado o backup.

5.5.2.2 Nos casos de cedência a outro órgão, desativar a conta durante o tempo de cedência.

5.6 Contas de correio eletrônico inativas por tempo superior a 6 (seis) meses devem ser desativadas, mediante notificação ao(à) magistrado(a)/servidor(a).

5.6.1 A notificação será realizada por meio do Sistema Eletrônico de Informação do PJRO.

5.6.2 Após o decorrer de 30 (trinta) dias do aviso, e não havendo manifestação, a conta poderá ser excluída, desde que realizado o procedimento de *backup.*

5.6.2.1 Nos casos de exclusão, deve-se informar à SGP e ao DECOM sobre o procedimento executado.

5.6.3 Os prazos de desativação e exclusão de contas de correio eletrônico podem ser reduzidos pontualmente mediante autorização do CGSI.

5.6.4 Não se aplicam a esses prazos, as contas de correio eletrônico que nunca fizeram *login* na ferramenta, podendo ser excluída pela STIC após 90 (noventa) dias da data da sua criação.

5.6.4.1 Nos casos de exclusão, será informado à SGP e ao DECOM sobre o procedimento executado, sem a necessidade de informação ao magistrado/servidor, ou mesmo, de realização de backup.

5.7 Poderá ser criada uma caixa postal institucional pessoal ao estagiário, caso seja solicitada formalmente pelo gestor da unidade, e seja necessária para desempenhar o serviço.

5.7.1 Aplicam-se aos estagiários as mesmas regras do 5.6 e disposições gerais.

5.8 Os casos omissos serão decididos pelo CGSI.

Seção II - Da Caixa Postal Institucional
Unidade/Comissão/Comitê/Grupo/Conselho

5.11 As unidades administrativas e judiciárias previstas na estrutura organizacional do PJRO, as comissões, os comitês, os grupos e os conselhos, poderão ter caixa postal institucional.

5.12 O gestor da unidade, presidente ou responsável pela comissão, comitê, grupo ou conselho será também o gestor da respectiva caixa postal, competindo-lhe:

5.12.1 Solicitar criação, alteração e exclusão da caixa postal institucional.

5.12.2 Gerenciar o compartilhamento de informações e o acesso de outros servidores, mediante delegação no sistema de correio eletrônico.

5.13 A caixa postal institucional, a que se refere o item 5.12, terá um único endereço de correio eletrônico, cujo identificador será formado pela denominação da unidade/comissão/comitê/grupo/conselho ou por sigla que permita a sua identificação.

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

5.15 Aplicam-se as mesmas regras do item 5.6 à unidade/comissão/comitê/grupo/conselho.

Seção III - Da Lista de Distribuição
Criação, alteração e exclusão

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

5.17 A criação de lista de distribuição pode ser solicitada pelo gestor da unidade a qual se destina.

5.17.1 A destinação de lista de distribuição que dependa de correios eletrônicos de outras unidades deverá ser autorizada pelos gestores das unidades receptoras.

5.17.2 A criação de lista de distribuição destinada a todos os correios eletrônicos do PJRO deverá ser autorizada pela Presidência do TJRO.

5.18 A solicitação deve ser encaminhada à Secretaria de Tecnologia da Informação e Comunicações (STIC), 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.

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

5.19.1 Manter permanentemente atualizado o rol de integrantes da lista de distribuição;

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

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

5.20 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.

Seção IV - Disposições Gerais

5.21 O acesso às mensagens está restrito ao remetente e ao destinatário, sendo estas invioláveis, salvo por determinação do CGSI.

5.22 Qualquer leitura indevida de mensagens de correios eletrônicos alheias, estará sujeita a possível responsabilização administrativa, cível e criminal.

5.23 A entrega de cópias dos arquivos e correios eletrônicos armazenados pelo PJRO, ao usuário desligado, será efetuada somente mediante autorização do CGSI.

5.24 São deveres e responsabilidades do usuário do correio eletrônico institucional:

5.24.1 Utilizar a conta de correio eletrônico institucional para a comunicação oficial, em detrimento da utilização de outros serviços semelhantes;

5.24.2 Sigilo quanto ao acesso e à guarda da credencial individual;

5.24.3 Não compartilhar as credencias de acesso do correio eletrônico com terceiros.

5.25 São deveres da STIC quanto ao monitoramento das contas de correio eletrônico:

5.25.1 Alertar os usuários quanto a eventual mau funcionamento ou interrupção do serviço de correio eletrônico;

5.25.2 Alertar o gestor responsável quanto a eventual má utilização do correio eletrônico por sua equipe, para as devidas providências quanto à aplicação de sanções cabíveis;

5.26 O período de retenção do backup deste normativo será estipulado pela "NSIC 10 - Backup e Restauração de Dados desta Política".

5.27 Recomenda-se, para uma melhor identificação do remetente, ao final de cada mensagem de correio eletrônico, incluir assinatura conforme sugestão a seguir:

Recomendação de formatação de assinatura nas mensagens de correio eletrônico.
"Nome do usuário" "Setor do usuário" Poder Judiciário do Estado de Rondônia Telefone(s)/Ramal (69) "9999"-"9999"

6 MONITORAMENTO E AUDITORIA

6.1 Por motivos de segurança, o serviço de correio eletrônico será monitorado, e os registros serão mantidos pela Secretaria de Tecnologia da Informação e Comunicação por no mínimo 6 (seis) meses e até 12 (doze) meses.

6.2 O monitoramento será 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 de TIC do PJRO ou que contenham conteúdo impróprio.

6.3 Em caso de indícios de descumprimento das diretrizes previstas neste normativo, o Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética (GPTIR) poderá de ofício ou por determinação do Comitê Gestor de Segurança da Informação e Cibernética (CGSI) realizar auditoria sobre os fatos.

6.4 Os relatórios decorrentes das auditorias ordinárias e extraordinárias realizadas pelo Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética serão encaminhados ao Comitê Gestor de Segurança da Informação, para análise e deliberação.

6.5 A Secretaria de Tecnologia da Informação e Comunicações (STIC) encaminhará até o dia 1 de dezembro de cada ano, relatório às unidades/comissões/comitês/grupos/conselhos e ao seu respectivo gestor, presidente ou responsável, com o rol das listas de distribuição e caixas postais a elas vinculadas, bem como a lista de eventuais caixas postais de estagiários.

6.6 Cabe ao gestor conferir os dados do relatório referido no item 6.5 e fazer os ajustes necessários até o dia 15 de dezembro do mesmo ano.

7 DISPOSIÇÃO FINAL

7.1 O disposto na presente norma será atualizado sempre que alterados os procedimentos e controles ou quando necessário, mediante iniciativa do CGSI.