



**Poder Judiciário do Estado de Rondônia
Gabinete da Presidência**

ANEXO XIII

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 11 - ACESSO AOS DATACENTERS

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



Poder Judiciário do Estado de Rondônia
Gabinete da Presidência

**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



**Poder Judiciário do Estado de Rondônia
Gabinete da Presidência**

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 11 - Acesso aos Datacenters				
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



**Poder Judiciário do Estado de Rondônia
Gabinete da Presidência**

Estabelecer diretrizes e padrões para o acesso aos datacenters do Poder Judiciário do Estado de Rondônia.

2 MOTIVAÇÃO

2.1 Disciplinar, por meio da conscientização e controles, o acesso a datacenters do PJRO.

2.2 Proteger a confidencialidade, integridade, disponibilidade e autenticidade das informações do PJRO;

2.3 Alinha-se às normas, regulamentações e melhores práticas relacionadas à matéria.

3 FUNDAMENTO 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 **Datacenter (Centro de Processamento de Dados):** é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e



**Poder Judiciário do Estado de Rondônia
Gabinete da Presidência**

sistemas de ativos de rede, como switches, roteadores e outros, considerado assim, o sistema nervoso dos dados da instituição.

4.2 Sala-Cofre: é ambiente físico estanque, testado e certificado que protege o datacenter do PJRO contra fogo, calor, umidade, gases corrosivos, fumaça, alagamentos, roubo, arrombamento, acesso indevido, sabotagem, impacto, pó, explosão, magnetismo e armas de fogo.

4.3 Sala Segura: ambiente que possui a finalidade de proteger os equipamentos e dados críticos de um datacenter contra danos causados por fogo, calor, gases e impactos.

4.4 Datacenter Externo: datacenter localizado fora da estrutura predial do PJRO, compartilhado por meio de convênio com órgãos públicos parceiros.

4.5 Sala de Telecom: sala com servidores e/o equipamentos de redes que interligam a rede corporativa do PJRO com as operadoras de telecom e a internet.

4.6 Salas de Racks de Rede: salas com os equipamentos de redes que interligam a rede corporativa do PJRO.

4.7 Ativos de Rede: equipamentos específicos que permitem estruturar uma rede de computadores, conectando as máquinas da instituição umas às outras e também conectando a organização à internet.

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

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

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

4.11 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.

5 CONTROLES

5.1 Os ambientes dos Datacenters do PJRO são compostos pelas seguintes áreas:

5.1.1 Sala Cofre: Sala UPS - Ala 1; Centro de Controle: Ala 2; Sala-Cofre: Ala 3; Corredor técnico: Ala 4;

5.1.1.1 Sala de Telecom;

5.1.2 Sala Segura: Sala Telecom - Ala 1; Sala UPS: Ala 2; Sala Segura: Ala 3;

5.1.3 Salas de Racks de Rede;

5.1.4 Salas de Telecom das Comarcas;



**Poder Judiciário do Estado de Rondônia
Gabinete da Presidência**

- 5.2 Em horário de funcionamento do PJRO, o acesso aos ambientes dos datacenters somente será realizado pelas pessoas credenciadas e autorizadas pela STIC e/ou DEA.
- 5.2.1 São automaticamente autorizados e credenciados a entrar nos ambientes dos datacenters:
- 5.2.1.1 Presidente do CGSI;
- 5.2.1.2 Diretor(a) do Desein;
- 5.2.1.3 Servidores lotados nas Divisões de Gerenciamento de Dados (Digid), de Infraestrutura (Dinfra) e de Segurança da Informação (Disein).
- 5.3 O pedido de acesso aos ambientes dos datacenters do PJRO será feito por meio de pedido de autorização formal para a STIC.
- 5.4 As pessoas autorizadas terão livre acesso ao ambiente, desde que o façam por meio do acesso biométrico.
- 5.5 No caso de desligamento de usuários que possuam acesso aos Datacenters, imediatamente deverá ser providenciada a sua exclusão da lista de usuários autorizados.
- 5.6 Todos os acessos aos datacenters do PJRO deverão ser registrados.
- 5.7 Todos os ambientes dos datacenters do PJRO deverão ser monitorados por câmeras.
- 5.8 Não é permitida a entrada com qualquer tipo de bebida, comida, produto fumígeno ou inflamável nos ambientes dos datacenters do PJRO.
- 5.9 É proibido a captura de imagem por vídeo ou fotografia dos ambientes dos datacenters do PJRO, sem a devida autorização da STIC.
- 5.10 Os ambientes dos datacenters deverão ser mantidos limpos e organizados. Qualquer procedimento que gere lixo ou sujeira nesses ambientes somente poderá ser realizado na presença de um(a) colaborador(a) da STIC.
- 5.11 Não é permitida a entrada e/ou a saída de peças, equipamentos e acessórios dos ambientes dos datacenters do PJRO, sem o prévio conhecimento e autorização da STIC.
- 5.12 O DEA tem acesso aos ambientes dos datacenters do PJRO para manutenção na rede lógica, elétrica e hidráulica.
- 5.13 O acesso aos ambientes dos datacenters do PJRO deverá ser feito por meio de biometria.
- 5.14 A STIC deverá designar as pessoas para o cadastramento biométrico nas portas de acesso aos ambientes dos datacenters do PJRO.
- 5.15 É de competência da STIC a geração de relatórios quando houver qualquer ocorrência nos ambientes dos datacenters do PJRO ou sempre que solicitado pela Administração do PJRO.



**Poder Judiciário do Estado de Rondônia
Gabinete da Presidência**

5.16 Para os casos de intervenções e serviços a serem realizados nos edifícios que impactem no funcionamento dos ambientes dos datacenters do PJRO, a STIC deve ser previamente notificada.

5.17 Fora do horário de expediente do PJRO, fins de semana e feriados, o acesso aos ambientes dos datacenters do PJRO somente será realizado para monitoramento, manutenções preventivas agendadas ou ações corretivas emergenciais, por pessoas credenciadas e autorizadas pela STIC.

5.18 Quando autorizado o acesso aos ambientes dos datacenters do PJRO, a liberação de acesso será feita remota ou localmente pela STIC, dependendo da necessidade de acompanhamento da atividade.

Seção I - Acesso aos Datacenters Externos

5.19 A STIC fornecerá ao órgão parceiro a lista dos servidores/magistrados que podem ter acesso aos datacenters.

5.20 O acesso ao datacenter será realizado pelas políticas dos órgãos parceiros conforme convênio estabelecido com o PJRO.

Seção II - Acesso a Salas de Telecom das Comarcas

5.21 O acesso de visitantes ou terceiros às Salas de Telecom das Comarcas, somente poderá ser realizado com acompanhamento de um servidor autorizado, e:

5.21.1 Caso haja necessidade das empresas terceirizadas adentrarem as salas de datacenter em horário extraordinário e na ausência de um técnico da STIC, o(a) administrador(a) local ou ainda o(a) supervisor(a) de segurança do Fórum, realizará o acompanhamento dos acessos às Salas de Telecom das comarcas.

5.21.2 Caso haja necessidade de acesso não emergencial, a área requisitante deve solicitar autorização com antecedência à STIC.

5.22 Serão permitidos nas Salas de Telecom das comarcas, somente equipamentos de TIC utilizados para a interligação das comarcas e serviços essenciais.

6 MONITORAMENTO E AUDITORIA



**Poder Judiciário do Estado de Rondônia
Gabinete da Presidência**

6.1 Por motivos de segurança, os acessos aos datacenters (logs de acesso e imagens) serão monitorados e os registros serão mantidos pela Secretaria de Tecnologia da Informação e Comunicação por, no mínimo, 6 (seis) meses e, no máximo, 12 (doze) meses.

6.1.1 O controle das imagens será realizado pela Coordenadoria de Segurança Patrimonial e Humana (COSEPH).

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.