



**TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO**  
Gabinete da Presidência

**RESOLUÇÃO GP N. 310, DE 15 DE DEZEMBRO DE 2023**

Altera a [Resolução GP n. 134, de 19 de dezembro de 2019](#), que institui a Política de Segurança da Informação e Comunicação do Tribunal Regional do Trabalho da 3ª Região (POSIC-TRT3).

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de atualização da [Resolução GP n. 134, de 19 de dezembro de 2019](#); e

CONSIDERANDO a importância de adotar boas práticas de segurança da informação e comunicação,

RESOLVE:

Art. 1º Esta Resolução altera a [Resolução GP n. 134, de 19 de dezembro de 2019](#), que institui a Política de Segurança da Informação e Comunicação do Tribunal Regional do Trabalho da 3ª Região (POSIC-TRT3).

Art. 2º A [Resolução GP n. 134, de 2019](#), passa a vigorar com as seguintes alterações:

*"Art. 9º Auditorias poderão ser realizadas pela Divisão de Segurança da Informação (DISI) e pela Diretoria de Tecnologia da Informação e Comunicação (DTIC) para apurar eventos que possam representar*

riscos à segurança da informação ou contrariar as boas práticas no uso dos recursos de TIC." (NR)

**"Seção II  
Da Divisão de Segurança da Informação**

Art. 13. Compete à DISI:

*I - elaborar minutas de normas de segurança da informação e encaminhá-las ao Comitê de Segurança da Informação e Proteção de Dados.*

.....

*III - prestar assessoramento e apoio técnico especializado ao Comitê de Segurança da Informação e Proteção de Dados, mantendo-o informado a respeito de incidentes de segurança da informação.*

....." (NR)

*"Art. 16. Compete à DISI a supervisão e o acompanhamento do cumprimento da POSIC-TRT3.*

....." (NR)

*"Art. 17. ....*

*Parágrafo único. As minutas de atos normativos resultantes dos trabalhos de revisão mencionados no **caput** serão apreciados pelo Comitê de Segurança da Informação e Proteção de Dados, após manifestação do Comitê de Tecnologia da Informação e Comunicação (CTIC)." (NR)*

*"Art. 19. Os casos omissos serão submetidos à deliberação do Comitê de Segurança da Informação e Proteção de Dados." (NR)*

Art. 3º O [Anexo I](#) da [Resolução GP n. 134, de 2019](#), passa a vigorar com as seguintes alterações:

**"NORMA COMPLEMENTAR N. 1  
EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES DE  
SEGURANÇA CIBERNÉTICA (ETIR)**

1. ....

*1.1. Coordenar as atividades de tratamento e resposta a incidentes de segurança cibernética no âmbito do Tribunal Regional do Trabalho da 3ª Região.*

2. ....

*2.1. O público-alvo da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) é formado pelos usuários do ambiente tecnológico deste Tribunal.*

**3. Integrantes**

*3.1. A ETIR é composta pelos seguintes integrantes:*

*3.1.1. o(a) diretor(a) de Tecnologia da Informação e Comunicação;*

*3.1.2. o(a) secretário(a) de Infraestrutura Tecnológica;*

*3.1.3. o(a) secretário(a) de Sistemas;*

*3.1.4. o(a) secretário(a) de Suporte e Atendimento;*

*3.1.5. o(a) chefe da Divisão de Segurança da Informação; e*

3.1.6. o(a) substituto(a) formalmente designado(a) será o(a) suplente de cada integrante.

3.2. A ETIR é coordenada pela Divisão de Segurança da Informação (DISI).

#### **4. Modelo de Implementação**

4.1. A ETIR poderá solicitar apoio de suas equipes ou apoio multidisciplinar de outras áreas organizacionais (jurídica, gestão de pessoas, comunicação social, etc.) para responder aos incidentes de segurança de maneira adequada e tempestiva.

4.2. Os membros da ETIR, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e à resposta a incidentes de segurança da informação.

#### **5. Autonomia**

5.1. A autonomia da ETIR é compartilhada. A equipe recomendará os procedimentos a serem executados ou as medidas de recuperação durante eventual incidente de segurança da informação e apresentará as ações a serem tomadas, ou as consequências se as recomendações não forem seguidas.

5.2. De acordo com a gravidade do incidente, a recomendação deverá, ainda, ser submetida ao Comitê de Segurança da Informação e Proteção de Dados e/ou à Presidência do Tribunal.

5.3. As ações serão sempre definidas em conjunto com as instâncias consultadas.

#### **6. Atribuições**

6.1. Propor ações de contenção para os incidentes de segurança da informação relacionados aos ativos de tecnologia da informação.

*6.2. Analisar as informações sobre vulnerabilidades, artefatos maliciosos e tentativas de intrusão, com definição de estratégias e ações para sua detecção ou correção.*

*6.3. Fornecer informações, aos envolvidos, sobre a ocorrência e, ao público interno, orientações de prevenção de incidentes de segurança da informação.*

*6.4. Propor divulgação de alertas ou advertências diante da ocorrência de eventual incidente de segurança da informação ou, de forma proativa, em face de vulnerabilidades e incidentes conhecidos e que possam gerar impactos nas atividades dos usuários.*

*6.5. Apoiar a execução do processo de gerenciamento de crise cibernética. (NR)*

Art. 4º Revogam-se os itens 4.3 a 4.8 do [Anexo I](#) da [Resolução GP n. 134, de 2019](#).

Art. 5º Esta Resolução entra em vigor na data de sua publicação.

**RICARDO ANTÔNIO MOHALLEM**  
Desembargador Presidente