PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DA 2ª REGIÃO

ATO GP Nº 02, DE 07 DE JANEIRO DE 2022

Redefine a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 2ª Região.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos deste Tribunal com integridade, confidencialidade e disponibilidade;

CONSIDERANDO que a credibilidade da instituição na prestação jurisdicional deve ser sempre preservada;

CONSIDERANDO a constante preocupação com a qualidade e celeridade na prestação de serviços à sociedade,

RESOLVE:

Art. 1º Redefinir a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 2ª Região.

Art. 2º Para os efeitos deste Ato aplicam-se as seguintes definições:

I - Confidencialidade: Garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

II - Integridade: Salvaguarda de exatidão e completeza da informação e dos métodos de processamento;

III - Disponibilidade: Garantia de que os (as) usuários (as) autorizados (as) obtenham acesso à informação e aos recursos correspondentes sempre que necessário;

IV - Autenticidade: Garantia da veracidade da fonte das informações, possibilitando confirmar a identidade da pessoa ou entidade que presta as informações;

V - Segurança da Informação: Preservação da confidencialidade, integridade e disponibilidade da informação;

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 02, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387 p. 6-9, 7 jan. 2022.

VI - Rede interna: Grupo de redes corporativas fornecidas e mantidas pelo Tribunal Regional do Trabalho da 2ª Região, tais como rede privada virtual - VPN, rede cabeada e redes sem fio destinadas ao público interno do Tribunal;

VII - Recurso de Tecnologia da Informação e Comunicações - TIC: Qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, ou as instalações físicas que os abriguem;

VIII - Usuários(as): Magistrados(as) e servidores(as) ocupantes de cargo efetivo ou em comissão, requisitados(as) e cedidos(as), empregados(as) de empresas prestadoras de serviços terceirizados, consultores(as), estagiários(as) e outras pessoas que, devidamente autorizadas, utilizem os recursos tecnológicos do Tribunal;

IX - Plano de Continuidade de Serviço de TIC: Documento com o objetivo de estabelecer os procedimentos necessários para restauração do funcionamento de um serviço de TIC no menor tempo possível, caso este serviço seja atingido por eventos que afetem sua disponibilidade;

X - Princípio do Menor Privilégio: Orientação para que qualquer tipo de acesso configurado seja realizado da forma mais restritiva possível, garantindo que:

a) o acesso seja concedido apenas às pessoas necessárias;

b) o acesso seja concedido apenas pelo tempo necessário;

c) o acesso seja concedido apenas aos recursos necessários;

d) o acesso seja concedido apenas aos perfis necessários.

XI - Registros de Auditoria (LOGS): Arquivos que contêm informações sobre eventos relevantes, como informações de autenticação ou de ações praticadas em equipamento ou serviço de TIC;

XII - Representante do Negócio: Pessoa ou comitê responsável por negociar com a comunidade de usuários(as) quais as regras, demandas, expectativas de nível de serviço e solicitações de mudanças devem ser feitas para os serviços e qual a prioridade destas;

XIII - Zona Desmilitarizada: Área reservada de rede de computadores responsável por concentrar os equipamentos que devem ser acessíveis por outras redes menos seguras, como a Internet, implementando regras de acesso específicas e suficientes para a proteção do ambiente computacional da instituição.

Art. 3º As disposições deste Ato aplicam-se a todos os(as) usuários(as) de recursos de TIC do Tribunal Regional do Trabalho da 2ª Região.

Art. 4º Compete ao(à) Gestor(a) de Segurança da Informação e Comunicações:

I - coordenar as atividades do Comitê de Segurança da Informação e Comunicações;

II - submeter à Presidência propostas de diretrizes, normas e políticas relativas à Segurança da Informação e Comunicações;

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 02, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387 p. 6-9, 7 jan. 2022.

III - promover a cultura de segurança da informação e comunicações;

IV - acompanhar os levantamentos e as avaliações dos danos decorrentes de quebra de segurança;

V - propor recursos necessários às ações de segurança da informação e comunicações;

VI - avaliar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações.

Art. 5º São atribuições da Coordenadoria de Segurança de TIC:

I - elaborar e coordenar ações relacionadas à segurança cibernética incluídas no Plano Diretor de TIC, com base nas definições estratégicas estabelecidas pelo Comitê de Segurança da Informação e Comunicações;

II - prestar apoio técnico especializado às atividades do Comitê de Segurança da Informação e Comunicações nos assuntos relacionados à Segurança de TIC;

III - informar ao Comitê de Segurança da Informação e Comunicações a respeito de incidentes de segurança de TIC e riscos identificados no ambiente computacional do Tribunal.

Art. 6º A Secretaria de Tecnologia da Informação e Comunicações implantará mecanismos de proteção que visem assegurar a confidencialidade, a integralidade e a disponibilidade do ambiente computacional do Tribunal.

Art. 7º Os registros de auditoria (logs) gerados nos equipamentos servidores devem ser armazenados em equipamento centralizado, com controles de acesso implementados de forma a garantir a integridade e a confidencialidade das informações.

Art. 8º As configurações de acesso ou comunicação realizadas nas soluções de infraestrutura e segurança de TIC devem obedecer ao princípio do menor privilégio.

§ 1º Qualquer acesso ou comunicação que não tenha necessidade de ser liberado deve ser bloqueado.

§ 2º Deverá ser implementada uma zona desmilitarizada para confinamento de equipamentos acessíveis publicamente através da internet.

§ 3º As redes que contêm equipamentos servidores devem ser segregadas das redes que contêm equipamentos de microinformática.

§ 4º A segregação das redes computacionais deve considerar as necessidades de isolamento e o nível de segurança adequado para cada ambiente, sistema ou unidade organizacional.

§ 5º As interfaces administrativas dos serviços de TIC devem ser disponibilizadas exclusivamente por meio da rede interna, considerando-se a utilização de autenticação com múltiplos fatores sempre que viável.

Art. 9º Sempre que viável, deverão ser utilizados protocolos de comunicação que implementem mecanismos de criptografia em detrimento de protocolos sem estes mecanismos.

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 02, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387 p. 6-9, 7 jan. 2022.

Parágrafo único. Deve ser considerada a utilização de recursos de soluções de criptografia, ampliando o uso de assinatura eletrônica, conforme legislações específicas.

Art. 10. A geração e restauração de cópias de segurança do ambiente computacional deverão seguir o disposto no Ato GP nº 07, de 23 de março de 2015.

Art. 11. O descarte seguro de mídias de armazenamento de dados no âmbito deste Tribunal deverá seguir o disposto no Ato GP nº 09, de 23 de março de 2015.

Art. 12. O uso adequado dos recursos de TIC visa garantir a continuidade da prestação jurisdicional e das atividades administrativas deste Tribunal.

§ 1º. Os recursos de tecnologia da informação, pertencentes ao Tribunal que estão disponíveis para os(as) usuários(as), devem ser utilizados em atividades relacionadas às suas funções institucionais.

§ 2º. A utilização dos recursos de TIC será monitorada, podendo serem realizadas auditorias com a finalidade de detectar eventos que deponham contra a segurança da informação e comunicações, as boas práticas no uso dos recursos de TIC ou eventos que estejam em desconformidade com os normativos vigentes.

§ 3º. A utilização dos recursos de TIC deverá seguir as diretrizes contidas no Ato GP nº 45, de 25 de setembro de 2018.

Art. 13. A Solução de Colaboração e Comunicação Corporativa deve ser utilizada como ferramenta institucional para execução das atribuições funcionais de magistrados(as) e servidores(as) ativos.

Parágrafo único. Assuntos relacionados à rotina de trabalho devem ser tratados exclusivamente através das contas corporativas de correio eletrônico, fornecidas por este Tribunal, sendo vedada a utilização de contas pessoais de correio eletrônico para este fim.

Art. 14. O serviço de acesso à Internet provido através da rede do Tribunal deve restringir-se às páginas com conteúdo estritamente relacionado com as atividades desempenhadas pelo Órgão, necessários ao cumprimento das atribuições funcionais do(a) usuário(a).

§ 1º O Comitê de Segurança da Informação e Comunicações deliberará a respeito de solicitações de acesso a sites bloqueados pela política de acesso vigente, mas que sejam necessários à rotina funcional das unidades solicitantes.

§ 2º Equipamentos fornecidos para utilização do público em geral terão regras de acesso específicas, de acordo com a necessidade de cada equipamento, elaboradas de acordo com o princípio do menor privilégio.

Art. 15. Toda informação gerada no Tribunal será classificada em termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento, observadas as diretrizes contidas no Ato GP nº 30, de 15 de dezembro de 2014.

Art. 16. As informações, sistemas e métodos gerados ou criados por magistrados(as) e servidores(as), no exercício de suas funções, independentemente da forma de sua apresentação ou armazenamento, são propriedades do Tribunal e serão utilizadas exclusivamente para fins corporativos.

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 02, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387 p. 6-9, 7 jan. 2022.

Art. 17. Quando informações, sistemas e métodos forem gerados ou criados por terceiros para uso exclusivo do Tribunal, ficam os criadores obrigados ao sigilo permanente de tais produtos, sendo vedada a sua reutilização em projetos para outrem.

Art. 18. Os contratos e convênios firmados pelo Tribunal que envolvam a utilização de recursos de TIC devem conter cláusulas contemplando os requisitos de segurança de TIC necessários à manutenção da integridade, confidencialidade, disponibilidade e autenticidade das informações.

§ 1º. Cabe ao(à) demandante de cada contratação identificar a necessidade de cláusulas para a manutenção da segurança do ambiente computacional, considerando o objeto pretendido.

§ 2º. Contratos que envolvam tratamento de dados pessoais devem prever os controles necessários para atendimento à Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018).

Art. 19. O gerenciamento da continuidade dos serviços de TIC será realizado mediante processo que deverá cobrir, no mínimo, as seguintes atividades:

I - elaboração de planos de continuidade de serviços de TIC;

II - revisão dos planos de continuidade de serviços de TIC;

III - testes dos planos de continuidade de serviços de TIC.

§ 1º Deverão ser elaborados planos de continuidade de serviços de TIC que contemplem, no mínimo, todos os serviços de TIC considerados críticos.

§ 2º Os planos de continuidade serão atualizados sempre que houver alteração no ambiente computacional ou nos procedimentos necessários para seu restabelecimento.

§ 3º. Deverá ser elaborado cronograma para execução de teste dos planos de continuidade de todos os serviços considerados críticos.

Art. 20. Os incidentes cibernéticos serão tratados conforme disposto na Política de Gerenciamento de Incidentes Cibernéticos.

Art. 21. Os(as) usuários(as) deverão notificar à Central de Serviços de TIC qualquer incidente de segurança de TIC identificado.

Art. 22. Os riscos de segurança de TIC serão tratados mediante processo que deverá cobrir, no mínimo, as seguintes atividades:

I - Definições preliminares: Definição do escopo priorizando, no mínimo, os ativos associados aos serviços considerados críticos;

II - Análise e avaliação: Identificação, comunicação, avaliação, aceitação e priorização dos riscos;

III - Plano de tratamento: Definição das formas de tratamento dos riscos que deve relacionar, no mínimo, as ações a serem tomadas, as pessoas responsáveis, as prioridades e os prazos de execução necessários à sua implantação;

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 02, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387 p. 6-9, 7 jan. 2022.

IV - Execução do plano de tratamento: Execução das ações previstas no plano de tratamento dos riscos aprovado;

V - Análise dos resultados: Avaliação dos resultados na execução do plano, contendo quais ações foram executadas, dificuldades encontradas na execução das ações e qualquer outra informação que seja relevante ao processo;

VI - Melhoria do processo: Avaliação da eficiência e eficácia do processo, e dos problemas encontrados durante sua execução, revisão das etapas e ações previstas, revisão do escopo para próximas análises e implementações de melhorias.

Art. 23. A conformidade técnica em segurança de TIC será gerenciada através do processo de Gerenciamento de Conformidade de TIC.

Art. 24. O controle de acesso aos serviços de TIC será gerenciado através do processo de Gerenciamento de Cumprimento de Requisição.

§ 1º O gerenciamento de identidades e controle de acesso lógico deverá seguir as diretrizes contidas no Ato GP nº 45, de 2018.

§ 2º Os acessos devem ser geridos através do princípio do menor privilégio.

§ 3º O(a) representante de negócio de cada serviço de TIC é responsável por definir as regras de acesso ao respectivo serviço.

§ 4º A criação ou alteração de credenciais de acesso deve seguir o disposto no Ato GP nº 08, de 23 de março de 2015, que institui a Política de Senhas no âmbito do Tribunal.

Art. 25. O acesso físico ao Datacenter e às instalações de TIC deverão seguir o disposto no Ato GP nº 10, de 23 de março de 2015.

Art. 26. A divulgação e conscientização em segurança de TIC será realizada mediante processo que deverá cobrir, no mínimo, as atividades de elaboração, revisão e divulgação de material sobre o tema.

Art. 27. Deverá ser estabelecido um programa de capacitação e conscientização em segurança de TIC, de forma que os(as) usuários(as) recebam informações apropriadas ao desempenho de suas funções.

§ 1º O programa deverá considerar as seguintes diretrizes:

I - ter por objetivo tornar os(as) usuários(as) conscientes das suas responsabilidades para a segurança da informação e comunicações e os meios pelos quais essas responsabilidades são realizadas;

II - estar alinhado com as políticas e procedimentos relevantes de segurança de TIC;

III - considerar um número mínimo de atividades de conscientização, tais como campanhas e notícias;

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 02, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387 p. 6-9, 7 jan. 2022.

IV - contemplar novos (as) usuários (as);

V - promover capacitação contínua para os(as) servidores(as) responsáveis pela manutenção da segurança cibernética do ambiente computacional do Tribunal.

§ 2º. Serão incluídas no Plano de Capacitação de TIC, no mínimo, 40 (quarenta) horas anuais de treinamentos para os(as) servidores(as) lotados(as) na Coordenadoria de Segurança de TIC, diretamente envolvidos(as) com a manutenção da segurança cibernética do ambiente computacional do Tribunal.

Art. 28. Todos os processos de segurança de TIC elaborados devem ser publicados na Intranet, para livre consulta.

Art. 29. Incumbe à chefia imediata do(a) servidor(a) verificar a observância desta Política, no âmbito de sua unidade, comunicando de imediato à Central de Serviços de TIC quaisquer irregularidades identificadas.

Parágrafo único. O descumprimento desta Política poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais.

Art. 30. A Política, as Normas e os Processos de Segurança da Informação e Comunicações deverão ser revisados e atualizados periodicamente, sempre que forem observadas mudanças significativas no ambiente organizacional ou computacional ou, no mínimo, a cada 12 (doze) meses.

Parágrafo único. A revisão deverá considerar, quando aplicável:

I - os resultados provenientes das análises de risco;

II - os relatórios sobre incidentes de segurança de TIC;

III - as seguintes referências normativas:

a) Instrução Normativa Nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

b) ABNT NBR ISO/IEC 27001:2013;

c) ABNT NBR ISO/IEC 27002:2013;

d) ABNT NBR ISO/IEC 27005:2019.

IV - os relatórios de conformidade operacional/normativa relacionados.

Art. 31. Ficam revogados:

I - o Ato GP nº 28, de 10 de dezembro de 2012;

II - o Ato GP nº 29, de 15 de dezembro de 2014;

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 02, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387 p. 6-9, 7 jan. 2022.

III - o Ato GP nº 06, de 23 de março de 2015; e

IV - o Ato GP nº 38, de 05 de setembro de 2018.

Art. 32 Este Ato entra em vigor na data de sua publicação.

Publique-se e cumpra-se.

São Paulo, data da assinatura eletrônica.

LUIZ ANTONIO M. VIDIGAL
Desembargador Presidente do Tribunal

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 02, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387 p. 6-9, 7 jan. 2022.