RICARDO HOFMEISTER DE ALMEIDA MARTINS COSTA
12/12/2024 15:35

PORTARIA GP.TRT4 Nº 4.742 DE 12 DE DEZEMBRO DE 2024.

Altera a Portaria GP.TRT4 nº 4.772/2008, que institui a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 4ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Portaria Presidência CNJ nº 140/2024, que determina a implementação do método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis;

CONSIDERANDO a revisão e atualização anual da Política de Segurança da Informação, conforme estabelece o artigo 1º, § 1º, da Portaria GP.TRT4 n° 4.772/2008;

CONSIDERANDO o que consta nos Processos Administrativos PROADs nºs 7248/2019, 7264/2019, 7268/2019 e 11519/2020,

RESOLVE:

Art. 1º Incluir "considerando" na Portaria GP.TRT4 nº 4.772/2008, com a seguinte redação:

> **CONSIDERANDO** o que consta no Processo Administrativo PROAD nº 7248/2019,

Art. 2º Alterar o artigo 14-C da Portaria GP.TRT4 nº 4.772/2008, que passa a vigorar com a seguinte redação:

> Art. 14-C. O tratamento de dados pessoais no âmbito deste Tribunal é regido pela Política de Proteção e Privacidade de Dados Pessoais do TRT-4, instituída por meio da Portaria nº GP.TRT4 2.036/2021.

Art. 3º Incluir o subitem 5.3.6 no Anexo 1 da Portaria 4.772/2008, com a seguinte redação:

> 5.3.6. Armazenar informações de trabalho em sítios e/ou serviços de armazenamento em nuvem que não sejam homologados pelo TRT4 ou autorizados pelo Comitê de Segurança da Informação e Proteção de

Dados.

Art. 4º Incluir os subitens 3.15, 4.4, 5.10 e 7.1.1 no Anexo 2 da Portaria 4.772/2008, com as seguintes redações:

> 3.15. Autenticação de multifator (MFA): é quando mais de um fator é utilizado em conjunto para autenticação do usuário. Por exemplo: senha pessoal mais senha de uso único (OTP - *One Time Password*).
> […]
> 4.4. Portaria CNJ nº 140/2024, que determina a implementação do método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis.
> […]
> 5.10. O acesso às caixas postais institucionais pessoais e de unidades se dará por meio de autenticação de multifator.
> […]
> 7.1.1. É vedada a utilização do endereço de correio eletrônico institucional para cadastro em sítios ou serviços de interesses particulares.

Art. 5º Alterar os subitens 5.7.1.6, 5.7.2.1, 7.4, 7.8.1 e 8.6 do Anexo 2 da Portaria GP.TRT4 4.772/2008, que passam a vigorar com as seguintes redações:

> 5.7.1.6. A caixa postal institucional pessoal de magistrados ou servidores será excluída definitivamente nos casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção, permuta de magistrado, vacância por posse em outro cargo inacumulável e requisição/cedência a outro órgão ou retorno à origem.
> […]
> 5.7.2.1. O gestor da unidade poderá solicitar, formalmente, à SETIC, a criação de caixa postal institucional pessoal ao estagiário somente quando houver essa necessidade para o serviço a ser desempenhado.
> […]
> 7.4. O tamanho máximo da mensagem eletrônica, incluindo os anexos, não pode exceder 25 megabytes (MB).
> […]
> 7.8.1. A SETIC não garante a recuperação de mensagens de e-mails ou de caixas postais excluídas há mais de 25 dias.

> […]
> 8.6. Cabe ao gestor conferir os dados do relatório referido no item anterior e, até o dia 15 de dezembro do mesmo ano, solicitar à SETIC os ajustes necessários.

Art. 6º Incluir os subitens 4.15, 4.16, 5.5.3.3 e 6.2.12 no Anexo 3 da Portaria GP.TRT4 nº 4.772/2008, com as seguintes redações:

> 4.15. Drive Individual: área de armazenamento em nuvem vinculado à caixa postal individual ou setorial.
> 4.16. Drive Compartilhado: área de armazenamento em nuvem destinada a uma unidade específica do Tribunal.
> […]
> 5.5.3.3. Softwares instalados em desacordo ao item 5.5.3 e subitens poderão ser removidos pela SETIC, sem prévio aviso ao usuário e sem a realização de cópia de segurança.
> […]
> 6.2.12. Por razões de segurança do ambiente tecnológico, contas de rede não utilizadas há, pelo menos, 12 meses poderão ser desabilitadas pela SETIC, sem aviso prévio.

Art. 7º Incluir o inciso V no subitem 6.2.5 do Anexo 3 da Portaria GP.TRT4 nº 4.772/2008, com a seguinte redação:

> V) não utilizar senhas iguais às utilizadas no TRT4 em outros sítios ou sistemas na internet.

Art. 8º Alterar os subitens 5.2.5.1, 6.1.1 e 6.1.6 do Anexo 3 da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

> 5.2.5.1. É permitida a conexão de dispositivos móveis particulares nas redes sem-fio administradas pelo TRT4, desde que por meio de autenticação que possibilite a identificação inequívoca do usuário.
> […]
> 6.1.1. Os acessos à rede, serviços e aos sistemas computacionais disponibilizados pelo TRT4 serão solicitados à Secretaria de Tecnologia da Informação e Comunicações, por meio do sistema de atendimento, ou diretamente em sistema próprio de gerenciamento de acessos, em que definidos os níveis de acesso adequados às atividades desenvolvidas.
> […]
> 6.1.6. As novas senhas solicitadas serão únicas e fornecidas por meio de comunicação eletrônica para a

caixa postal institucional da unidade ou caixa postal institucional pessoal do usuário, proibido o fornecimento de senhas por qualquer outro meio, inclusive telefone.

Art. 9º Alterar o subitem 5.3 do Anexo 3 da Portaria GP.TR4 nº 4.772/2008, que passa a vigorar com a seguinte redação:

5.3. **Nuvem corporativa**
5.3.1. Ao armazenamento de arquivos na nuvem corporativa aplicam-se as regras previstas no subitem 5.2.6.
5.3.2. A SETIC não garante a recuperação de caixas postais, mensagens de e-mails e arquivos armazenados na solução em nuvem excluídos há mais de 25 dias.
5.3.3. É vedado armazenar informações de trabalho em sítios e/ou serviços de armazenamento em nuvem que não sejam homologados pelo TRT4 ou autorizados pelo Comitê de Segurança da Informação e Proteção de Dados.
5.3.4 *Drive* Individual
5.3.4.1. É recomendado que os arquivos armazenados no *drive* individual sejam vinculados (ter como proprietário) à caixa postal institucional da unidade, quando existente, ou outra designada pelo gestor da unidade para tal fim.
5.3.4.2. Nos casos de relotação ou afastamentos previstos no Anexo 2 desta Política (casos de exclusão da caixa postal), o gestor deverá solicitar ao servidor ou estagiário, de forma antecipada, sempre que possível, a verificação da existência de arquivos que digam respeito às atividades da unidade e que permaneçam na propriedade do servidor/estagiário, para que sejam transferidos para o *drive* compartilhado da unidade ou outra designada pelo gestor.
5.3.4.2.1. Caso persistam arquivos vinculados ao *drive* individual do servidor/estagiário quando de sua exclusão, eles serão transferidos para o *drive* compartilhado da unidade, ou outra designada pelo gestor, para triagem e definição da necessidade ou não de manutenção dos arquivos.
5.3.4.3. Nos casos de exclusão do *drive* individual de magistrados (exceto a hipótese de falecimento), será dada ciência, de forma antecipada, sobre a necessidade de transferência ou *download* dos arquivos armazenados na nuvem, sob pena de serem excluídos juntamente com a caixa postal individual.

5.3.4.4. Nos casos de exclusão da caixa postal institucional de unidade, os arquivos serão transferidos para a conta da unidade designada como nova responsável pelas atividades ou para servidor designado para tal fim.
5.3.5. *Drive* Compartilhado
5.3.5.1. Cada unidade do TRT4 terá disponível uma área de armazenamento em d*rive* compartilhado para salvaguardar os arquivos relacionados ao trabalho desenvolvido, com garantia de integridade, disponibilidade e com cópia de segurança.
5.3.5.1.1. O armazenamento do *drive* compartilhado será limitado em até 500.000 arquivos.
5.3.5.1.2. Em caso de necessidade de armazenamento superior ao limite estabelecido no item anterior, o gestor da unidade deverá encaminhar solicitação, formal, à SETIC para avaliar e autorizar a criação de novo *drive* compartilhado para a unidade;
5.3.5.2. A responsabilidade sobre o conteúdo armazenado no *drive* compartilhado é de responsabilidade do gestor da unidade para a qual o *drive* compartilhado foi designado.
5.3.5.3. O gerenciamento da permissão de acessos do *drive* compartilhado é de responsabilidade do gestor da unidade para a qual o *drive* compartilhado foi designado.
5.3.5.4. O compartilhamento de arquivos armazenados no *drive* compartilhado deve ser realizado exclusivamente com autorização do gestor da unidade.

Art. 10. Incluir o subitem 4.9 no Anexo 6 da Portaria GP.TRT4 nº 4.772/2008, com a seguinte redação:

4.9. Portaria GP.TRT4 nº 3.360/2023, que institui o Plano de Gestão de Riscos do TRT4.

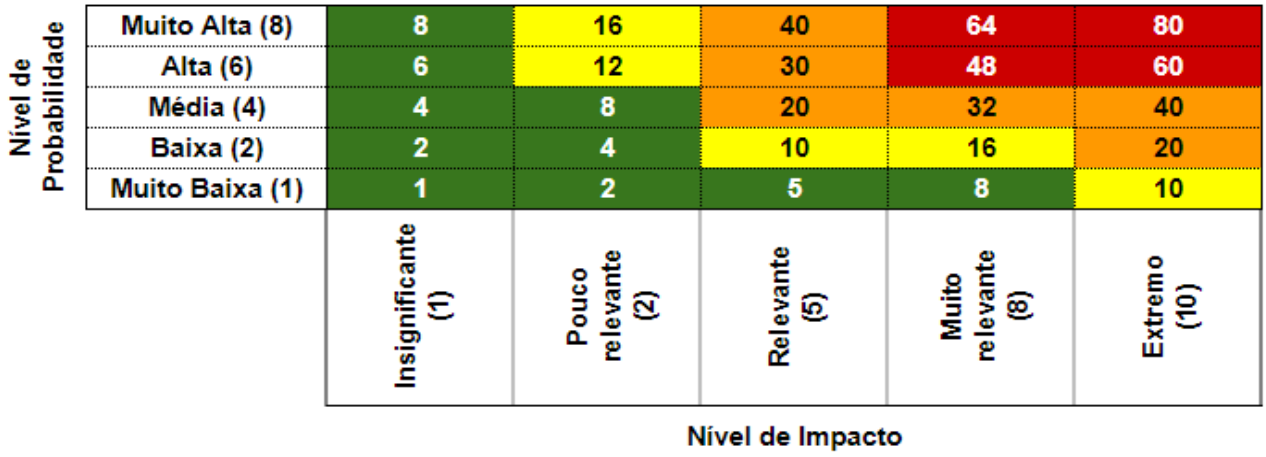
Art. 11. Alterar os subitens 7.1, 9.1, 10.2, 10.5.1 e 10.5.2 do Anexo 6 da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

7.1. A Gestão de Riscos leva em consideração as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TIC e está alinhada à Política de Segurança da Informação e à Política de Gestão de Riscos Institucional.
[…]
9.1. A gestão de riscos em processos de TIC é definida na especificação de cada processo e visa à

> identificação e ao tratamento dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria. As atividades inerentes à gestão de riscos nos processos de TIC devem observar as diretrizes desta norma e outras específicas relacionadas ao processo.
> […]
> 10.2 O processo de GRSIC-TRT4 está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2019 e ABNT NBR ISO/IEC 31000:2018, na Instrução Normativa GSI/PR nº 3 e da Portaria GP.TRT4 nº 3.360/2023.
> […]
> 10.5.1. Contextualização - compreende o mapeamento dos ativos, a definição e aprovação do contexto da análise e avaliação de riscos a ser realizada, com a identificação de seu propósito, escopo, limites e partes interessadas.
> 10.5.2. Análise e Avaliação dos Riscos - compreende a identificação, análise e avaliação dos riscos, bem como a elaboração e aprovação do Plano de Tratamento dos Riscos.

Art. 12. Alterar o subitem 10.3 do Anexo 6 da Portaria GP.TRT4 nº 4.772/2008, que passa a vigorar com a seguinte redação:

> 10.3. Os riscos serão avaliados a partir da: a) **Probabilidade**, que é a possibilidade de algum evento adverso ocorrer, podendo gerar impacto negativo. A escala é definida em cinco níveis: Muito baixa, Baixa, Média, Alta e Muito Alta; b) **Impacto**, que é a medida do dano ocasionado caso o evento adverso concretize-se. A escala é definida em cinco níveis: Insignificante, Pouco relevante, Relevante, Muito relevante e Extremo. Dessa forma os riscos são analisados com base em duas variáveis (probabilidade e impacto). O produto dessas duas variáveis determina o nível do risco, conforme mapa a seguir:



Classificação do Risco	Valores do RISCO
Risco Baixo	inferior a 10
Risco Médio	entre 10 e 19,99
Risco Alto	entre 20 e 44,99
Risco Extremo	superior a 45

Art. 13. Revogar o subitem 9.2 do Anexo 6 da Portaria GP.TRT4 nº 4.772/2008.

Art. 14. Alterar o subitem 7.14 do Anexo 8 da Portaria GP.TRT4 nº 4.772/2008, que passa a vigorar com a seguinte redação:

> 7.14. O encerramento do incidente de segurança da informação será realizado pelo coordenador da ETIR, com comunicação a todas as áreas interessadas e ao Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.BR) na forma e nos casos definidos pelo referido órgão.

Art. 15. Incluir o subitem 4.13 no Anexo 10 da Portaria GP.TRT4 nº 4.772/2008, com a seguinte redação:

> 4.13. Sistema de Gestão de Segurança da Informação (SGSI) - processo que representa a gestão do Macroprocesso de Gestão de Segurança da Informação, englobando todas as atividades realizadas pela Coordenadoria de Segurança da Informação e Proteção de Dados para um biênio.

Art. 16. Alterar os subitens 6.1.1, 6.1.2 e 6.1.4 do Anexo 10 da Portaria GP.TRT4 4.772/2008, que passam a vigorar com as seguintes redações:

> 6.1.1. Planejamento - compreende a avaliação da necessidade de criação, exclusão ou revisão dos planos

já instituídos, seja em virtude do tempo decorrido desde sua aprovação, seja em razão de mudanças no ambiente tecnológico, procedimentos ou testes realizados.
6.1.2. Execução - abrange a elaboração ou revisão dos planos pelas equipes técnicas, com a descrição dos cenários de falhas e os procedimentos técnicos para lidar com os problemas, a aprovação dos planos, seu armazenamento e divulgação; além da realização de testes dos Planos.
[…]
6.1.4. Encerramento - compreende a análise dos incidentes críticos ocorridos (desastres), a identificação das oportunidades de melhoria e seu encaminhamento à consideração superior, via SGSI, com vistas a dar início a novo ciclo do processo.

Art. 16. Revogar o subitem 6.1.3 do Anexo 10 da Portaria GP.TRT4 nº 4.772/2008.

Art. 17. Republique-se a Portaria GP.TRT4 nº 4.772/2008, com as alterações ora promovidas.

Art. 18. Esta Portaria entra em vigor na data de sua publicação.

Documento assinado digitalmente
RICARDO HOFMEISTER DE ALMEIDA MARTINS COSTA
Presidente do TRT da 4 Região