PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DA 2ª REGIÃO

ATO GP Nº 65, DE 21 DE OUTUBRO DE 2024

Redefine a Política de Senhas, 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 o Ato GP nº 02, de 7 de janeiro de 2022, que redefine a Política de Segurança da Informação, no âmbito do Tribunal Regional do Trabalho da 2ª Região – TRT-2;

CONSIDERANDO a Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça – CNJ, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário – ENSEC-PJ;

CONSIDERANDO os Protocolos e Manuais aprovados pela Portaria nº 162, de 10 de junho de 2021, do CNJ;

CONSIDERANDO a necessidade de estabelecer critérios para a criação de senhas, com o objetivo de aumentar a segurança das usuárias, dos usuários e do ambiente computacional do TRT-2,

RESOLVE:

Art. 1º A Política de Senhas, no âmbito do Tribunal Regional do Trabalho da 2ª Região – TRT-2, fica redefinida nos termos deste Ato.

Art. 2º As seguintes definições são válidas para os efeitos previstos na Política de Senhas:

I - credencial de acesso, no escopo deste ato normativo, é o mesmo que senha;

II - macros correspondem à ação ou a um conjunto de ações automatizadas, disparadas por algum comando de entrada;

III - teclas de função são teclas configuradas para executar automaticamente algum comando ao serem acionadas;

IV - autenticidade é a propriedade que assegura que uma informação foi produzida, emitida ou modificada por uma determinada pessoa ou sistema legitimado para tal finalidade;

V - senhas administrativas são senhas que habilitam a determinados usuários o acesso com privilégios administrativos a equipamentos que integram a infraestrutura computacional do TRT-2;

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 65, de 21 de outubro de 2024. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 4084, p. 1-4, 21 out. 2024.

VI - recursos correspondem ao equipamento ou à aplicação de infraestrutura tecnológica responsável pelo processamento e armazenamento de informações utilizadas pelo TRT-2;

VII - privilégios administrativos são os privilégios de acesso irrestrito, destinados à administração de determinado recurso e não apenas à sua simples utilização;

VIII - confidencialidade é a propriedade que assegura que uma informação é acessada apenas por pessoa credenciada para tal acesso;

IX - integridade é a propriedade que assegura que uma informação não foi modificada ou destruída indevidamente;

X - criptografia é a técnica que consiste em tornar um texto claro e legível em texto codificado e não legível, garantindo a confidencialidade da informação;

XI - função criptográfica *hash* é uma técnica que converte uma informação legível como, por exemplo, uma senha, em um código irreversível, garantindo a confidencialidade da informação; e

XII - técnica de *salt* é uma técnica segundo a qual é adicionado um valor único à senha antes da aplicação da função criptográfica, de maneira que duas senhas idênticas gerem códigos diferentes.

Art. 3º As disposições deste Ato aplicam-se a todas as usuárias e usuários de recursos de tecnologia da informação do TRT-2.

Art. 4º As senhas de acesso à rede corporativa são de uso pessoal e intransferível.

Parágrafo único. A usuária ou o usuário é responsável por:

I - manter sigilo sobre suas credenciais de acesso; e

II - qualquer ação realizada com suas credenciais de acesso no ambiente computacional do TRT-2.

Art. 5º A política de acesso a determinado recurso tecnológico, com ou sem a utilização de senha, é definida pelo Comitê de Segurança da Informação e Proteção de Dados Pessoais – CSIPDP.

Art. 6º Não é permitido tentar obter ou conseguir acesso não autorizado em qualquer sistema informatizado ou equipamento do ambiente computacional do TRT-2.

Art. 7° As senhas devem atender a parâmetros mínimos de complexidade, visando impossibilitar a sua descoberta por meios técnicos ou por adivinhação.

§ 1º A Secretaria de Tecnologia da Informação e Comunicações manterá a lista de parâmetros mínimos de complexidade das senhas pública e atualizada na Intranet, para livre consulta.

§ 2º As senhas geradas automaticamente por sistemas informatizados devem utilizar a maior complexidade possível no referido sistema, em relação à quantidade de caracteres e presença de outros grupos de caracteres, como símbolos, letras acentuadas ou sinais de pontuação.

Art. 8º É recomendável que todas as senhas atendam às boas práticas de segurança da informação, ou seja:

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 65, de 21 de outubro de 2024. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 4084, p. 1-4, 21 out. 2024.

I - não devem conter, em todo ou em parte, nome do usuário ou sua matrícula institucional;

II - não devem conter datas;

III - não devem conter informações pessoais;

IV - não devem conter informações de fácil dedução;

V - não devem ser armazenadas em papel ou em qualquer outro meio que facilite sua descoberta por outras pessoas; e

VI - não devem ser incluídas em processos automáticos, como macros ou teclas de função.

Art. 9º As senhas de usuárias e usuários de recursos sob responsabilidade exclusiva do TRT-2 terão validade máxima de um ano, devendo ser alteradas antes do término desse período.

§ 1º A Secretaria de Tecnologia da Informação e Comunicações enviará mensagem de correio eletrônico às usuárias e usuários cujas senhas estejam prestes a expirar, com antecedência mínima de um mês em relação à data de validade.

§ 2º Findo o prazo do *caput* sem a alteração da senha, as usuárias e usuários terão suas senhas desabilitadas e deverão utilizar os mecanismos de recuperação de senha disponibilizados pela Secretaria de Tecnologia da Informação e Comunicações.

§ 3º Durante a troca de senhas, as usuárias e usuários não poderão escolher senha já utilizada anteriormente.

Art. 10. As usuárias e usuários poderão trocar suas senhas a qualquer tempo, antes da expiração do prazo estabelecido no *caput* do art. 9º, ocasião em que a validade da senha será renovada por um ano.

Parágrafo único. Quando for solicitada a intervenção da Secretaria de Tecnologia da Informação e Comunicações para alteração de uma senha, a solicitação deverá ser realizada pela própria usuária ou usuário, que se submeterá a um processo para verificação de autenticidade de perfil.

Art. 11. As senhas das usuárias e usuários serão desabilitadas temporariamente sempre que houver tentativas excessivas de acesso mal sucedido em um curto período de tempo.

Art. 12. As senhas das usuárias e usuários que não acessarem o ambiente corporativo por longos períodos, conforme parâmetros definidos pelo TRT-2, serão desabilitadas automaticamente.

Parágrafo único. Na hipótese prevista no *caput,* a usuária e o usuário deverão providenciar a alteração de sua senha conforme previsto nos §§ 2º e 3º do art. 9º.

Art. 13. As senhas administrativas serão gerenciadas por meio de solução de gestão de acesso privilegiado (Privileged Access Management – PAM), que empregará os controles de segurança necessários para garantir a confidencialidade, integridade e disponibilidade das senhas.

§ 1º Sempre que tecnicamente viável, senhas administrativas deverão ser atribuídas a usuárias e usuários específicos e individuais.

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 65, de 21 de outubro de 2024. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 4084, p. 1-4, 21 out. 2024.

§ 2º As senhas administrativas devem ser dedicadas para as atividades que requeiram acesso privilegiado, sendo vedado seu uso para atividades rotineiras como navegação na *internet*, utilização de correio eletrônico ou atividades similares.

§ 3º O acesso aos ativos de infraestrutura utilizando senhas administrativas deverá ser realizado por meio da solução de PAM, sendo vedado o acesso direto aos ativos, salvo em situações excepcionais para resolução de problemas ou incidentes cibernéticos.

§ 4º Salvo nos eventuais casos de restrições impostas pela solução tecnológica utilizada, nenhum recurso deve entrar em operação antes que seja feita a alteração da senha administrativa padrão do fabricante.

Art. 14. As senhas das unidades são de responsabilidade da gestora ou do gestor da respectiva unidade.

Parágrafo único. O compartilhamento da senha da unidade deve ser evitado e não afasta a responsabilidade da gestora ou do gestor da unidade sobre o respectivo uso.

Art. 15. As bases de dados que armazenam senhas devem protegê-las mediante o emprego de função criptográfica *hash* e, sempre que possível, da técnica de *salt*, de modo que não seja possível a qualquer pessoa, mesmo que seja da equipe técnica de tecnologia da informação do TRT-2, recuperar a senha armazenada.

Art. 16. Os sistemas informatizados sob responsabilidade exclusiva do TRT-2 deverão prover mecanismos que garantam que qualquer nova senha esteja em conformidade com os critérios definidos nesta Política.

Parágrafo único. Os mecanismos que implementam os critérios definidos nesta Política poderão ser auditados pela Secretaria de Tecnologia da Informação e Comunicações, a qualquer tempo, para verificação dos controles empregados.

Art. 17. Ficam revogados:

I - o Ato GP nº 8, de 23 de março de 2015; e

II - o Ato GP nº 26, de 6 de junho de 2022.

Art. 18. Este Ato entra em vigor na data de sua publicação.

Publique-se e cumpra-se.

São Paulo, data da assinatura eletrônica.

VALDIR FLORINDO
Desembargador Presidente do Tribunal

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 65, de 21 de outubro de 2024. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 4084, p. 1-4, 21 out. 2024.