Norma de controle de acesso lógico

1 Objetivo

1.1 Estabelecer controles de acesso lógico com o objetivo de garantir que:

- apenas usuários autorizados tenham acesso aos ativos de informação;
- os usuários tenham acesso apenas aos recursos realmente necessários para a execução de suas tarefas;
- o acesso a recursos críticos seja monitorado e restrito a poucas pessoas;
- os usuários estejam impedidos de executar transações incompatíveis com sua função.

1.2 O controle de acesso pode ser traduzido, então, em termos de funções de identificação e autenticação de usuários; alocação, gerência e monitoramento de privilégios; limitação, monitoramento e desabilitação de acessos; e prevenção de acessos não autorizados.

2 Referências legais e normativas

- Brasil. Tribunal de Contas da União. Boas práticas em segurança da informação / Tribunal de Contas da União. – 4. ed. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.
- Conselho Nacional de Justiça. Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário, de junho de 2012.
- GSI/PR. Norma Complementar 07/IN01/DSIC/GSIPR, de julho de 2014.

3 Diretrizes

3.1 Quanto à criação e administração de contas de acesso

3.1.1 A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento para todo usuário.

3.1.2 O usuário, que não possui direitos e privilégios de administração de rede, terá somente uma única conta institucional de acesso, pessoal e intransferível.

3.1.3 Apenas usuários cadastrados para execução de tarefas específicas na administração de ativos de informação poderão ter conta de acesso no perfil de administrador.

3.1.4 O usuário será responsabilizado pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso.

3.1.5 A criação de contas de serviço se dará por meio de processo automatizado.

3.1.6 O Gestor de Serviço de TIC é responsável por estabelecer regras para credenciamento, perfil de acesso, bloqueio e exclusão de contas de seus usuários e das unidades

subordinadas ao sistema do qual ele é o responsável.

3.1.7 A autenticação de multifatores deve ser adotada, sempre que possível, para o controle de acesso lógico, a fim de autenticar a identidade de um usuário e vinculá-lo a uma conta de acesso a ativos de informação.

3.1.8 A obtenção, renovação ou revogação de Certificados Digitais válidos no âmbito da ICP-Brasil seguem as regras estabelecidas pelas Autoridades Certificadoras e de Registros a ela subordinadas.

3.1.9 O modo de definição e funcionamento de senhas de acesso será definida em norma específica.

3.1.10 As solicitações de criação, alteração e exclusão de qualquer tipo de acesso lógico devem ser encaminhadas para a Secretaria de Tecnologia de Informação e Comunicações (SETIC), por intermédio da Central de Serviços de TIC.

3.2 Quanto à rede corporativa de computadores

3.2.1 As credenciais de acesso à rede corporativa de computadores serão concedidas após a data de contratação ou de entrada em exercício do usuário.

3.2.2 As credenciais de acesso à rede corporativa de computadores serão desativadas quando houver encerramento do vínculo do usuário com a Instituição.

3.2.3 A SETIC será responsável pela manutenção das contas de acesso à rede corporativa.

3.2.4 O TRT pode autorizar acesso à rede corporativa de computadores para prestadores de serviços terceirizados, mediante solicitação justificada pelo Gestor do Contrato ou previsão contratual, sendo que a SETIC a submeterá, quando for o caso, ao Comitê de Segurança da Informação.

3.2.5 Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, quando do término de contrato ou após a realização do serviço prestado que motivou a solicitação, devendo o bloqueio ser solicitado pelo Gestor do Contrato.

3.2.6 Os acessos, identificados com login e senha, à rede corporativa, sejam locais ou remotos, serão registrados de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo de 2 anos.

3.2.7 Mecanismos, na rede corporativa, serão mantidos contendo os elementos possíveis e necessários para identificar endereços e serviços utilizados.

3.2.8 Para a concessão de acesso às informações sigilosas, será utilizada a legislação específica.

3.3 Quanto aos ativos de informação

3.3.1 Cada ativo de informação terá um Gestor, sendo tarefa deste estabelecer e providenciar a

execução das regras para credenciamento, perfil de acesso, bloqueio e exclusão de contas dos usuários ao ativo de informação sob sua guarda e representantes de outros órgãos públicos.

3.3.2 O TRT pode autorizar acesso aos ativos de informação aos prestadores de serviços terceirizados, mediante solicitação justificada pelo Gestor do Contrato ao Gestor do ativo, que a submeterá, quando for o caso, ao Comitê de Segurança da Informação.

3.3.3 Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, quando do término de contrato ou após a realização do serviço prestado que motivou a solicitação, devendo o bloqueio ser solicitado pelo Gestor do Contrato.

3.3.4 Ferramentas de proteção que favoreçam, preferencialmente, a administração de forma centralizada, serão utilizadas contra acesso não autorizado aos ativos de informação

3.3.5 Observar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação.

3.3.6 Registrar e permitir auditoria de eventos relevantes para a segurança e rastreamento de acesso às informações sigilosas.

3.3.7 O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade pública será considerado indevido e passível de imediato bloqueio temporário de acesso por parte da SETIC, que submeterá ao Comitê de Segurança da Informação para apreciação da situação, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.