MINISTÉRIO DA CULTURA

GERENCIAMENTO DE ACESSO DO USUÁRIO

ORIGEM

Ministério da Cultura – MinC.

REFERÊNCIAS LEGAIS E NORMATIVAS

Portaria nº 327/2014/MinC - Aprova, no âmbito do Ministério da Cultura, norma de Segurança que estabelece as Diretrizes de Segurança da Informação e Comunicações.

Portaria nº 119/2011/MinC - Institui a Política de Segurança da Informação e Comunicações do Ministério da Cultura e o Sistema de Segurança da Informação e Comunicações e dá outras providências.

Portaria nº 40/2013/MinC – Aprova o Regimento Interno do Ministério da Cultura.

ABNT ISO GUIA 73:2009 – Gestão de Riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação.

ABNT NBR ISO/IEC 27002:2007 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação.

ABNT NBR ISO/IEC 38500:2009 – Governança Corporativa de Tecnologia da Informação.

07/IN01/DSIC/GSIPR – Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal - APF, direta e indireta.

CAMPO DE APLICAÇÃO

Este documento se aplica no âmbito do Ministério da Cultura – MinC.

SUMÁRIO

APROVAÇÃO

Comitê de Segurança da Informação e Comunicações - CSIC

1. OBJETIVO

1.1 Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.

2. ESCOPO

2.1 Dispor sobre as regras para a criação e administração de contas e senhas de acesso aos recursos de tecnologia da informação e rede local do MinC.

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos servidores e colaboradores que exercem função de administração dos recursos de tecnologia da informação da rede corporativa, doravante chamados simplesmente de administradores de recursos de tecnologia da informação, sendo de responsabilidade de cada um o seu cumprimento.

4. CONCEITOS E DEFINIÇÕES

4.1 Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações estão conceituados no Dicionário de Referência.

5. PRINCÍPIOS

5.1 A Política de Segurança da Informação e Comunicações está fundamentada nos princípios da disponibilidade, integridade, confidencialidade e autenticidade, visando à proteção e à preservação das informações necessárias às atividades da instituição.

6. REGISTRO DE USUÁRIO

6.1 Disponibilizar ao usuário, que não exerce funções de administração da rede corporativa, somente uma única conta de acesso, pessoal e intransferível (Ref. NC 07/IN01/DSIC/GSIPR).

6.2 Utilizar conta de acesso no perfil de administrador de rede, pessoal e intransferível, somente para usuários cadastrados para execução de tarefas específicas na administração de recursos de tecnologia da informação que compõem a rede corporativa (Ref. NC 07/IN01/DSIC/GSIPR).

6.3 Deve ser estabelecido um gerenciamento rígido das credenciais ou contas de acesso e privilégios atribuídos por meio de um procedimento formal de registro para garantir os acessos em todos os recursos de tecnologia da informação, sistemas de informação e serviços de TI, atendendo minimamente aos seguintes requisitos e procedimentos:

a) solicitação formal e motivada:

- do chefe imediato ou superior do usuário à área responsável pela gestão de pessoas, que encaminhará o pedido à área responsável pela administração dos recursos de tecnologia da informação para criação de conta de acesso definitiva à rede corporativa e ao correio eletrônico corporativo;
- da área solicitante à área responsável pela administração dos recursos de tecnologia da informação para a criação de conta de acesso temporária à rede corporativa e ao correio eletrônico corporativo;
- da área solicitante ao proprietário do ativo de informação para criação de conta de acesso definitiva aos sistemas de informação; e
- da área solicitante ao proprietário do ativo de informação para criação de conta de acesso temporária aos sistemas de informação.

b) formação da conta de acesso pelo CPF do usuário, conforme a nomenclatura definida e padronizada pela área responsável pela administração dos recursos de tecnologia da informação;
c) credencial ou conta de acesso única para assegurar a responsabilidade de cada usuário por suas ações;
d) permissões de acesso limitadas àquelas estritamente necessárias para a execução de suas atividades;
e) permissão do uso de grupos de credenciais ou contas de acesso somente onde existe necessidade para o negócio ou por razões operacionais;
f) declaração por escrito dos direitos e deveres de acesso a ser fornecida aos usuários;
g) confirmação do usuário indicando que as condições de acesso foram entendidas;
h) liberação do acesso aos usuários somente após conclusão dos procedimentos de autorização; e
i) registro formal de todas as pessoas com direito de acesso concedido.

6.4 O cadastro único e atualizado com os dados das contas de acesso de usuários é reponsabilidade:

a) da área responsável pela gestão de pessoas juntamente com a área responsável pela administração dos recursos de tecnologia da informação nas contas de acesso à rede corporativa e ao correio eletrônico corporativo; e
b) do proprietário do ativo de informação nas contas de acesso aos sistemas de informação.

6.5 A conta de acesso do usuário deve ser bloqueada:

a) automaticamente, após 5 (cinco) tentativas de acesso mal sucedidas;
b) automaticamente, quando as senhas das contas de acesso não forem alteradas, no mínimo, a cada 90 (noventa) dias;
c) condicionalmente, quando solicitado pelo chefe imediato ou superior do usuário, formalmente justificado;

d) condicionalmente, quando solicitado pelo chefe imediato ou superior do usuário nas mudanças de suas atribuições, principalmente quando ocorrer o seu remanejamento para outra área;
e) condicionalmente, por solicitação da área responsável pela gestão de pessoas quando do afastamento do usuário em decorrência de processo administrativo; e
f) temporariamente, sempre que houver suspeita de que a utilização da conta esteja infringindo a Política de Segurança da Informação e Comunicações.

6.6 O desbloqueio da conta de acesso somente deve ser realizado mediante solicitação formal e motivada:

a) do chefe imediato ou superior do usuário à área responsável pela administração dos recursos de tecnologia da informação para as contas de acesso definitivas à rede corporativa; e
b) da área solicitante ao proprietário do ativo de informação para as contas de acesso definitivas aos sistemas de informação.

6.7 No desligamento de um usuário do MinC, o cancelamento da sua conta de acesso deverá ser formalmente solicitado:

a) pelo seu chefe imediato ou superior à área de gestão de pessoas que informará a área responsável pela administração dos recursos de tecnologia da informação sobre a autorização para exclusão da conta de acesso definitiva à rede corporativa; e
b) pela área solicitante ao proprietário do ativo de informação que efetuará o devido cancelamento da conta de acesso definitiva aos sistemas de informação.

7. GERENCIAMENTO DE PRIVILÉGIOS

7.1 A concessão e uso de privilégios deve ser restrita e controlada, evitando o uso inapropriado de privilégios especiais de acesso (quaisquer características ou recursos que habilitam usuários a exceder os controles existentes em sistemas e serviços), atendendo minimamente os seguintes requisitos e procedimentos:

a) identificar e registrar os privilégios especiais de acesso associados a cada componente relacionado ao uso de sistemas de informação e aplicações (sistema operacional, gerenciador de banco de dados, etc.);
b) identificar e registrar as categorias e perfis de usuários para os quais os privilégios especiais de acesso precisam ser concedidos;
c) conceder privilégios especiais de acesso a usuários conforme sua necessidade de uso e em concordância com a norma de Controle de Acesso à Rede;
d) conceder privilégios especiais de acesso somente após a conclusão dos procedimentos de autorização formal; e

e) registrar as concessões e alterações de privilégios especiais de acesso (como, por exemplo, no remanejamento de funcionários e prestadores de serviço) para posterior análise crítica.

7.2 Os privilégios especiais de acesso devem ser atribuídos para uma credencial ou conta de acesso diferente daquelas usadas normalmente pelo usuário.

7.3 A concessão de privilégios especiais de acesso deve ser sempre baseada no princípio da necessidade de conhecer, que determina o mínimo necessário para o desempenho das atribuições do usuário.

7.4 Deve ser estimulado o desenvolvimento e uso de sistemas que não precisem de privilégios especiais para seu funcionamento rotineiro (por exemplo, evitar que um sistema de contabilidade só acesse os bancos de dados caso os usuários tenham privilégios de administrador).

8. GERENCIAMENTO DE SENHA DO USUÁRIO

8.1 A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal, que atenda minimamente aos seguintes requisitos e procedimentos:

a) configurar sistemas de informação e serviços de TI para o correto tratamento de senhas, incluindo:

- senha com tamanho mínimo de 8 caracteres, sendo pelo menos 3 (três) deles numéricos ou especiais, obedecendo aos padrões mínimos de segurança definidos pela área responsável pela administração dos recursos de tecnologia da informação;
- exigência de troca de senha em intervalos não superiores a 90 (noventa) dias; e
- impedimento, quando da alteração, do uso das últimas senhas registradas e nem repeti-las no prazo de 30 (trinta) dias.

b) verificar a identidade do usuário antes de fornecer uma senha temporária, de substituição ou nova;
c) obter confirmação do usuário em declaração solicitando a manutenção da confidencialidade das senhas fornecidas, por meio do Termo de Responsabilidade do Usuário da Rede;
d) fornecer inicialmente aos usuários senhas seguras e temporárias com troca obrigatória no primeiro acesso realizado, considerando:

- as senhas temporárias devem ser diferentes a cada solicitação e não podem ser de fácil memorização.
- as senhas temporárias devem ser fornecidas de forma segura, evitando o uso de correio eletrônico de terceiros ou mensagens em texto claro.

e) os usuários devem acusar o recebimento das senhas.
f) manter senhas gravadas somente em recursos de tecnologia da informação protegidos.

9. ANÁLISE CRÍTICA DOS DIREITOS DE ACESSO DE USUÁRIO

9.1 Um processo formal de revisão periódica deve ser efetuado pela área responsável pela administração dos recursos de tecnologia da informação com o intuito de manter o controle efetivo sobre os direitos de acesso fornecidos aos usuários que atenda, pelo menos, aos seguintes requisitos e procedimentos:

a) revisão geral a cada 12 (doze) meses para usuários comuns;
b) revisão nos privilégios especiais de acesso a cada 4 (quatro) meses para constatar se privilégios não autorizados foram obtidos;
c) revisão específica e individualizada depois de qualquer mudança nos direitos de usuários (alteração da situação funcional ou do cargo, ou desligamento); e
d) revisão específica e individualizada por solicitação do Chefe imediato ou superior do usuário;
e) revisão de dados cadastrais, a cada 60 (sessenta) dias, para verificação e atualização de informações.

9.2 As contas de acesso não utilizadas por períodos superiores a 75 (setenta e cinco) dias serão automaticamente bloqueadas.

9.3 Deve ser verificada periodicamente a existência de credenciais ou contas de acesso redundantes, devendo ser inativadas ou bloqueadas. Credenciais ou contas de acesso redundantes não devem ser atribuídas a outros usuários.

10. PENALIDADES

10.1 Todos os servidores e colaboradores estão sujeitos às regras da Política de Segurança da Informação e Comunicações e devem observar integralmente o que dispõe este documento. A inobservância dessas regras acarretará em apuração das responsabilidades funcionais na forma da legislação em vigor, podendo haver responsabilização administrativa, civil e penal.

11. COMPETÊNCIAS E RESPONSABILIDADES

11.1 Os servidores e os colaboradores devem ter conhecimento da Política de Segurança da Informação e Comunicações, tendo a obrigação de seguir rigorosamente o disposto nas normas de segurança.

12. DISPOSIÇÕES GERAIS

12.1 Qualquer dúvida ou sugestões sobre a Política de Segurança da Informação e Comunicações e suas orientações devem ser imediatamente encaminhadas à área responsável por Segurança da Informação para análise e/ou esclarecimento.

13. ATUALIZAÇÃO

13.1 Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

14. VIGÊNCIA

14.1 Esta Norma entra em vigor na data de sua publicação.