PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

DIRETRIZES PARA IMPLEMENTAÇÃO DE CONTROLES DE ACESSO RELATIVOS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES.

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA LEGAL E NORMATIVA

Art. 6º da Lei nº 10.683, de 28 de maio de 2003;
Art. 8º do Anexo I do Decreto nº 6.931, de 11 de agosto de 2009;
Decreto nº 3.505, de 13 de junho de 2000;
Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008 e suas Normas Complementares;
NBR ISO/IEC 27001:2006 – Sistema de Gestão de segurança da informação;
NBR ISO/IEC 27002:2005 – Código de Práticas para a Gestão da Segurança da Informação;

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Anexo: Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1. OBJETIVO

Estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.

2. CONSIDERAÇÕES INICIAIS

2.1.O objetivo do controle é sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações.

2.2.A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso nos órgãos ou entidades da APF.

2.3.A identificação dos controles de acesso lógico e físico, nos órgão ou entidade da APF, é consequência do processo de Gestão de Riscos de Segurança da Informação e Comunicações.

2.4.A implementação dos controles de acesso está condicionada à prévia aprovação pela autoridade responsável pelo órgão ou entidade da APF.

2.5.Para implementar os controles de acesso aprovados é fundamental a elaboração e divulgação de normas, bem como programas periódicos de sensibilização e conscientização em conformidade com a Política de Segurança da Informação e Comunicações dos órgãos ou entidades da APF.

2.6.Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras específicas para credenciamento de acesso de usuários aos ativos de informação em conformidade com a legislação vigente, e em especial quanto ao acesso às informações em áreas e instalações consideradas críticas.

3. FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações - DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

4. CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

4.1. **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

4.2.**Ativos de informação** - os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

4.3.**Bloqueio de acesso**: processo que tem por finalidade suspender temporariamente o acesso.

4.4.**Contas de Serviço**: contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, script, etc.) sem qualquer intervenção humana no seu uso.

4.5.**Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

4.6.**Credenciamento**: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.

4.7.**Credenciais ou contas de acesso**: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.

4.8.**Exclusão de acesso**: processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso.

4.9.**Gestão de Riscos de Segurança da Informação e Comunicações** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

4.10. **Necessidade de conhecer** - condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.

4.11. **Perfil de acesso**: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

4.12. **Prestador de serviço**: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso.

4.13. **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;

4.14. **Termo de Responsabilidade**: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso (Modelo - Anexo A).

4.15. **Tratamento da informação**: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

4.16. **Usuário**: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade.

5. DIRETRIZES PARA CONTROLE DE ACESSO LÓGICO

5.1 Quanto à criação e administração de contas de acesso:

5.1.1 A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento para qualquer usuário.

5.1.2 Disponibilizar ao usuário, que não exerce funções de administração da rede local, somente uma única conta institucional de acesso, pessoal e intransferível.

5.1.3 Utilizar conta de acesso no perfil de administrador somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

5.1.4 Responsabilizar o usuário pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso, mediante assinatura de Termo de Responsabilidade (Modelo - Anexo A).

5.1.5 A criação de contas de serviço exige regras específicas vinculadas a um processo automatizado.

5.1.6 Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para credenciamento, bloqueio e exclusão de contas de acesso de seus usuários, bem como para o ambiente de desenvolvimento.

5.2 Quanto à rede corporativa de computadores:

5.2.1 Conceder credenciais de acesso à rede corporativa de computadores após a data de contratação ou de entrada em exercício do usuário.

5.2.2 Excluir credenciais de acesso à rede corporativa de computadores quando do desligamento do usuário.

5.2.3 Registrar os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em cada órgão ou entidade da APF.

5.2.4 Implementar, sempre que possível, pelo menos um dos mecanismos que contemplam biometria, tokens, smart cards, a fim de autenticar a identidade do usuário da rede.

5.2.5 Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores.

5.2.6 Manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.

5.2.7 Utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.

5.2.8 Gravar o acesso remoto à rede corporativa em logs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada;

5.2.9 Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para o uso de redes sem fio.

5.3 Quanto aos ativos de informação:

5.3.1 Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada.

5.3.2 Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;

5.3.3 Utilizar ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia;

5.3.4 Registrar eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas.

5.3.5 Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

5.3.6 O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade públicas será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.

5.3.7 Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para o uso da Internet, do Correio Eletrônico e de Mensagens Instantâneas.

6. DIRETRIZES PARA CONTROLE DE ACESSO FÍSICO

6.1 Quanto às áreas e instalações físicas:

6.1.1 Os Órgãos ou entidades da APF estabelecem regras para o uso de credenciais físicas (crachá, botom, cartões, selos, etc,), que se destinam ao controle de acesso dos usuários às áreas e instalações sob suas responsabilidades;

6.1.2 Os Órgãos ou entidades da APF definem a necessidade e orientam a instalação de sistemas de detecção de intrusos nas áreas e instalações sob suas responsabilidades;

6.1.3 Classificar as áreas e instalações como ativos de informação de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações, mapeando aquelas áreas e instalações consideradas críticas;

6.1.4 Os Órgãos ou entidades da APF orientam o uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída;

6.1.5 Proteger os ativos de informação contra ações de vandalismo, sabotagem, ataques, etc, especialmente em relação àqueles considerados críticos.

6.1.6 Implementar área de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais;

6.1.7 Definir pontos de entrega e carregamento de material com acesso exclusivo ao pessoal credenciado;

6.1.8 Intensificar os controles para as áreas e instalações consideradas críticas em conformidade com a legislação vigente.

6.2 Quanto aos usuários:

6.2.1 Difundir e exigir o cumprimento da Política de Segurança da Informação e Comunicações, das normas de segurança e da legislação vigente acerca do tema;

6.2.2 Conscientizar o usuário para adotar comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações.

6.2.3 Identificar e avaliar sistematicamente os riscos à segurança da informação e comunicações dos ativos de informação e quais controles devem ser aplicados quanto aos acessos dos usuários;

6.2.4 Estabelecer formulário específico de Termo de Responsabilidade (Modelo - Anexo A) a ser difundido e assinado individualmente pelos usuários;

6.2.5 Definir regras específicas para autorização de acesso e credenciamento dos usuários em conformidade com a classificação dos ativos de informação.

6.3 Quanto aos ativos de informação:

6.3.1 Estabelecer distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (backups);

6.3.2 Classificar os ativos de informação em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base a gestão de risco e a gestão de continuidade de negócios relativas aos aspectos da segurança da informação e comunicações da APF,

6.3.3 Um exemplo para classificação dos ativos de informação está disposto no Anexo B.

6.3.4 Os ativos de informação classificados como sigilosos requerem procedimentos especiais de controles de acesso físico em conformidade com a legislação vigente.

6.4 Quanto ao perímetro de segurança:

6.4.1 Definir perímetros de segurança, suas dimensões, equipamentos e tipos especiais de controles de acesso aos ativos de informação;

6.4.2 Ilustrar em documentação própria e permitir que sejam identificados os perímetros de segurança de cada ativo de informação por todos que transitarem ou tiverem acesso em tais espaços, em especial às áreas e instalações consideradas críticas;

6.4.3 Regulamentar, por intermédio de normas específicas de cada órgão ou entidade da APF, o armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetros de segurança.

7 VIGÊNCIA

Esta norma entra em vigor na data de sua publicação.

ANEXO A – Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL

(Nome do órgão ou entidade da APF)

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____deste (Nome do órgão ou entidade), DECLARO , sob pena das sanções cabíveis nos termos da _____ (legislação vigente) que assumo a responsabilidade por:

I) tratar o(s) ativo(s) de informação como patrimônio do (Nome do órgão ou entidade);

II) utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do (Nome do órgão ou entidade);

III) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

IV) utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do (Nome do órgão ou entidade);

V) responder, perante o (Nome do órgão ou entidade), pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

Local, UF, _____de _____de _____ .

_____

Assinatura

Nome do usuário e seu setor organizacional

_____

Assinatura

Nome da autoridade responsável pela autorização do acesso

ANEXO B - Modelo de Classificação de Ativos de Informação

Grau de criticidade	Ativos de informação	Impacto	Cor
Nível 1 – Alto	Data-center, servidores, central telefônica, recursos criptológicos, cópias de segurança, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de primeiro escalão.	Interrompe a missão do órgão ou provoca grave dano à imagem institucional, à segurança do estado ou sociedade.	Vermelha
Nível 2 – Médio	Computadores com dados e informações únicas, de grande relevância, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de segundo escalão.	Degrada o serviço do órgão ou provoca dano à imagem institucional, à segurança do estado ou sociedade.	Amarela
Nível 3 – Baixo	Os demais ativos de informação	Compromete planos ou provoca danos aos ativos de informação.	Sem cor