Ministério da Transparência, Fiscalização e Controladoria-Geral da União

REGULAMENTA OS CONTROLES DE ACESSO RELATIVOS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NO ÂMBITO DO MINISTÉRIO DA TRANSPARÊNCIA, FISCALIZAÇÃO E CONTROLADORIA-GERAL DA UNIÃO e dá outras providências.

ORIGEM

Comitê Permanente de Segurança Corporativa/COPESEG do Ministério da Transparência, Fiscalização e Controladoria-Geral da União

REFERÊNCIA NORMATIVA

Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 e Norma Complementar 07/IN01/DSIC/GSIPR, de 06/05/2010.
Portaria SE/CGU/PR nº 1214, de 03/06/2014
Instrução Normativa SE/CGU/PR nº 04, de 03/06/2014.

CAMPO DE APLICAÇÃO

Esta Norma se aplica no âmbito do Ministério da Transparência, Fiscalização e Controladoria-Geral da União.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

GILSON LIBÓRIO DE OLIVEIRA MENDES
Coordenador do Comitê Permanente de Segurança Corporativa

1 OBJETIVO

Disciplinar os controles de acesso relativos à Segurança da Informação e Comunicações nas unidades do Ministério da Transparência, Fiscalização e Controladoria-Geral da União.

2 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto na IN04/SE/CGU/PR, de 03 de junho de 2014, compete ao Ministério da Transparência, Fiscalização e Controladoria-Geral da União, por meio do Comitê Permanente de Segurança Corporativa/COPESEG, promover e propor normas e diretrizes quanto ao uso de recursos de tecnologia da informação no que diz respeito à Segurança Corporativa.

3. CONSIDERAÇÕES INICIAIS

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

3.2 A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso nas unidades da CGU;

3.3 A identificação dos controles de acesso lógico e físico na CGU é consequência do processo de Gestão de Riscos de Segurança da Informação e Comunicações;

3.4 A implementação dos controles de acesso está condicionada à prévia aprovação pela autoridade responsável em cada unidade da CGU;

3.5 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 da CGU.

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar, aplicam-se os seguintes termos 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 Controle de Acesso Lógico: o conjunto de procedimentos, recursos e meios utilizados com a finalidade proteger os ativos organizacionais baseados em tecnologia da informação contra acessos indevidos, bem como permitir acesso aos usuários legítimos desses ativos;

4.7 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;

4.8 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;

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

4.10 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;

4.11 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;

4.12 Perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

4.13 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;

4.14 Quebra de segurança: ação ou omissão, intencional ou acidental, que resulte no comprometimento ou no risco de comprometimento de informação sigilosa, em especial as classificada em qualquer grau de sigilo.

4.15 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);

4.16 Tratamento da informação: ***c***onjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação, inclusive as sigilosas;

4.17 Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação da CGU, formalizada por meio da assinatura do Termo de Responsabilidade.

5 DIRETRIZES PARA CONTROLE DE ACESSO LÓGICO

Caberá à Diretoria de Sistemas e Informação/DSI, apoiada pelo COPESEG, a observância das seguintes diretrizes:

5.1 Quanto à criação e administração de contas de acesso:

5.1.1 Criar e manter contas de acesso aos ativos de informação e implementar 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 Controlar as credenciais e os privilégios de acesso dos usuários aos ativos de tecnologia da informação da CGU, que deverão sempre espelhar sua situação funcional frente ao órgão, devendo ser concedidas, alteradas ou revogadas sempre que esta se modificar;

5.1.4 Implantar e manter a integração entre os sistemas de gerenciamento de usuários da área de Recursos Humanos e as bases de credenciais de acesso aos ativos de tecnologia da informação, visando minimizar inconsistências;

5.1.5 Monitorar os privilégios de acesso, que deverão se limitar ao mínimo necessário para que o usuário possa desempenhar adequadamente suas funções;

5.1.6 Observar que a concessão de privilégios deve, sempre que possível, utilizar o conceito de papéis, agrupando os privilégios de acordo com as responsabilidades exercidas;

5.1.7 Limitar a utilização de conta de acesso no perfil de administrador somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação;

5.1.7.1 A concessão de credenciais com perfil de administrador deverá sempre ser registrada, de modo a permitir auditoria;

5.1.8 Manter informado o usuário de que poderá ser responsabilizado pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso, exigindo-se previamente à concessão de acesso a assinatura de Termo de Responsabilidade (Anexo A);

5.1.9 Atentar que a criação de contas de serviço deverá observar regras específicas vinculadas a um processo automatizado;

5.1.10 Estabelecer, quando necessário, regras adicionais para credenciamento, bloqueio e exclusão de contas de acesso de seus usuários, bem como para o ambiente de desenvolvimento;

5.1.11 Manter informado o usuário de que é de sua responsabilidade, dentre outros aspectos:

5.1.11.1 A utilização idônea de sua credencial de acesso aos ativos de tecnologia da informação da CGU;

5.1.11.2 O encerramento da sessão de trabalho ou seu bloqueio com senha ao afastar-se do equipamento de trabalho;

5.1.11.3 A manutenção do sigilo de sua credencial de acesso aos ativos de tecnologia da informação da CGU;

5.1.11.4 A segurança das informações por ele manuseadas através dos ativos de tecnologia da informação da CGU;

5.1.11.5 Todos os acessos realizados aos ativos de tecnologia da informação da CGU através de sua credencial de acesso.

5.2 Quanto à rede corporativa de computadores:

5.2.1. A rede corporativa deverá ser segmentada em perímetros lógicos levando em consideração tanto ao requisito de disponibilidade dos serviços oferecidos quanto aos riscos de segurança da informação que está sujeita;

5.2.2 A concessão de credenciais de acesso à rede corporativa de computadores somente poderá ser aprovada após a contratação ou a entrada em exercício do usuário;

5.2.3 A exclusão de credenciais de acesso à rede corporativa de computadores deverá ocorrer quando do desligamento do usuário;

5.2.4 O registro dos acessos à rede corporativa de computadores será feito de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido pela Diretoria de Sistemas e Informação/DSI;

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

5.2.6. A conexão à rede corporativa deverá ser restrita aos equipamentos autorizados pela Diretoria de Sistemas e Informações - DSI/CGU;

5.2.6.1 Deverão ser estabelecidos, sempre que possível, mecanismos para identificação de equipamentos conectados à rede;

5.2.6.2 Os pontos de acesso físico à rede corporativa deverão ser controlados, e deverão permanecer habilitados apenas quando necessário.

5.2.6.3 Implementar, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados;

5.2.7 Aprovar 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 Controlar e guardar o acesso remoto à rede corporativa em logs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada;

5.2.9 Aprovar regras adicionais para o uso de redes sem fio.

5.3 Quanto aos ativos de informação:

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

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

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

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

5.3.7. O acesso a qualquer ativo de tecnologia de informação da CGU somente deve ser realizado por usuários credenciados e mediante processo de autenticação do usuário, autorização de acordo com privilégios previamente concedidos, bem como registro para fins de auditoria/monitoramento;

5.3.7.1 Todo acesso lógico a ambiente de rede externo realizado por meio de ativos de tecnologia da informação da CGU deverá ser igualmente autorizado, identificado e registrado.

5.3.7.2 Os ativos de tecnologia da informação devem ter sua confidencialidade e integridade garantidas, além de estar disponíveis para seus legítimos usuários no momento em que precisam ser acessados;

5.3.8. O acesso a qualquer ativo de tecnologia de informação da CGU poderá ser suspenso temporariamente, e sem aviso prévio, sempre que houver indícios de incidentes relacionados a controles de acesso aos ativos de tecnologia da informação até que seja verificada a situação e descartada a hipótese de incidente.

5.3.9 Exceções às disposições contidas neste documento, bem como os casos omissos e tecnologias específicas como uso de Internet, do Correio Eletrônico e de Mensagens Instantâneas, serão tratadas pela DSI/CGU;

6. DIRETRIZES PARA CONTROLE DE ACESSO FÍSICO

Caberá à Diretoria de Gestão Interna/DGI, apoiada pelo COPESEG, a observância das seguintes diretrizes:

6.1 Quanto às áreas e instalações físicas:

6.1.1 Estabelecer regras para o uso de credenciais físicas (crachá, *bottom*, cartões, selos, etc,), que se destinam ao controle de acesso dos usuários às áreas e instalações sob suas responsabilidades;

6.1.2 Definir a necessidade e orientar 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 Implementar 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 Implantar e manter 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 a exigência de cumprimento da Política de Segurança da Informação e Comunicações, das normas de segurança e da legislação vigente acerca do tema;

6.2.2 Promover a conscientização para adoção de comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações;

6.2.3 Identificar e avaliar sistemática dos 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 Implantar o uso de 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 Promover a classificação dos 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 CGU, tomando como exemplo para classificação dos ativos de informação o modelo disposto no Anexo B;

6.3.3 Observar que 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 Promover a ilustração em documentação própria e permissão para 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, o armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetros de segurança.

7 VIGÊNCIA

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

ANEXO A – Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL

Ministério da Transparência, Fiscalização e Controladoria-Geral da União/CGU

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF nº _____, Cédula de Identidade nº _____, expedida pelo _____, em _____, e lotado na _____ deste Ministério da Transparência, Fiscalização e Controladoria-Geral da União/CGU , 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 Ministério da Transparência, Fiscalização e Controladoria-Geral da União/CGU;

II) utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da CGU;

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 da CGU;

V) responder, perante a CGU, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

Cidade/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 da CGU 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 conectividade ou de armazenamento de informações ou de computação móvel das autoridades de segundo escalão.	Degrada o serviço da CGU 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