MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS
PROCURADORIA-GERAL DE JUSTIÇA

PORTARIA NORMATIVA Nº 933 , DE 7 DE AGOSTO DE 2014

Regulamenta o Acesso à Informação no âmbito do Ministério Público do Distrito Federal e Territórios.

A **PROCURADORA-GERAL DE JUSTIÇA DO MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS, em exercício,** no uso das atribuições legais conferidas pela Lei Complementar nº 75, de 20 de maio de 1993,

CONSIDERANDO o disposto na Portaria Normativa PGJ nº 177, de 12 de julho de 2011, que regulamenta a Política de Segurança da Informação - PSI no âmbito do Ministério Público do Distrito Federal e Territórios - MPDFT e institui o Comitê Gestor de Segurança da Informação;

CONSIDERANDO a Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011), que dispõe sobre o acesso a informações;

CONSIDERANDO a Resolução nº 89 do Conselho Nacional do Ministério Público, que regulamenta a Lei de Acesso à Informação no âmbito do Ministério Público da União e dos Estados;

CONSIDERANDO a Norma Complementar nº 07 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, de 06 de maio de 2010, intitulada "Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações";

CONSIDERANDO o disposto na Portaria Normativa PGJ nº 35, de 30 de janeiro de 2009, que dispõe sobre as atividades administrativas relacionadas à segurança orgânica no Ministério Público do Distrito Federal e Territórios e dá outras providências;

RESOLVE:

Art. 1º O acesso à informação será regido por esta Portaria Normativa, a qual será denominada Norma de Controle de Acesso à Informação – NCA.

Art. 2º A NCA tem por objetivo sistematizar a concessão de acesso e estabelecer diretrizes e requisitos de segurança no acesso físico e lógico às informações no âmbito do MPDFT.

Parágrafo Único. Estão submetidos à NCA todos os membros, servidores, estagiários, prestadores de serviço e demais agentes públicos ou privados que, por força de contratos, convênios, acordos de cooperação e instrumentos congêneres exerçam atividades no âmbito do MPDFT, bem como qualquer pessoa que venha a ter acesso a seus ativos de informação.

Art. 3° Considera-se, para fins desta Portaria Normativa, os seguintes termos, além daqueles citados na Portaria Normativa PGJ nº 177, de 12 de julho de 2011:

I. **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;

II. **Contas de Serviço**: contas de acesso à Rede de Informática do MPDFT necessárias a um procedimento automático (aplicação, script, etc.) sem qualquer intervenção humana no seu uso;

III. **Credenciamento**: processo pelo qual o colaborador 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;

IV. **Credencial**: permissão, concedida por autoridade competente após o processo de credenciamento, que habilita 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;

V. **Necessidade de conhecer**: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para ter acesso à informação, bem como o acesso aos ativos de informação;

VI. **Perfil de acesso**: conjunto de atributos de cada colaborador, definido previamente como necessário para credencial de acesso;

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

VIII. **Termo de Responsabilidade**: termo assinado pelo colaborador 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 no Anexo A);

IX. **Tratamento da informação**: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação;

X. **Ativo de Informação**: meios que produzem, processam, transmitem ou armazenam informações, aplicando-se subsidiariamente o disposto na Portaria

Normativa PGJ nº 177, de 12 de julho de 2011, que regulamenta a Política de Segurança da Informação – PSI, em seu artigo 2º;

XI. **Datacenter**: sala segura, sala-cofre, central de processamento de dados, sala de equipamentos de telecomunicações e/ou outros locais onde ficam ligados os equipamentos, servidores de rede, switches, roteadores e outros, responsáveis pelo funcionamento da rede de informática.

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 4º É assegurado a todos o direito fundamental de acesso à informação classificada como **ostensiva**, bem como a sua disponibilidade, autenticidade e integridade, observados os princípios básicos da administração pública, da inviolabilidade da vida privada e da intimidade e a Lei de Acesso a Informação.

Art. 5º Deve ser assegurado o controle de acesso às **informações sigilosas e às informações pessoais** sob custódia do MPDFT, observada a sua disponibilidade, confidencialidade, autenticidade e integridade.

Parágrafo único. O direito e a necessidade de conhecer, além da identificação do requerente, são condicionantes prévias para a concessão de acesso.

Art. 6º É assegurado o direito fundamental de acesso à informação classificada como **pessoal**, mediante autorização da autoridade responsável pela guarda da informação e as seguintes medidas de controle:

I. O acesso restrito à pessoa a que se referirem e a agentes públicos legalmente autorizados, independente da classificação de sigilo;
II. O acesso por parte de terceiros desde que legalmente autorizados, por ordem judicial ou consentimento expresso da pessoa a que se referirem.

Art. 7º A aquisição ou contratação de serviços para o fornecimento de sistemas de informação devem incorporar nos projetos a garantia dos controles apropriados, com base nas normas e requisitos de segurança do MPDFT, bem como na análise de riscos.

CAPÍTULO II
DO ACESSO FÍSICO À INFORMAÇÃO

Art. 8º Devem ser aplicados controles de acesso físico aos ativos de informação de acordo com a sua classificação e o grau de sigilo.

§ 1º Devem ser definidos pontos de entrega e carregamento de material e de acesso exclusivo ao pessoal credenciado.

§ 2º A área de recepção deve possuir regras claras para a entrada e saída de pessoas, equipamentos e materiais.

Art. 9º Compete à Coordenadoria de Segurança Institucional - CSI propor soluções que atendam ao previsto no artigo anterior, bem como implementá-las e monitorá-las.

CAPÍTULO III
DAS DIRETRIZES DE ACESSO FÍSICO AO DATACENTER

Art. 10. O Datacenter deve possuir as seguintes características de segurança física da informação:

I. Perímetro claramente estabelecido;
II. Uso exclusivo para instalação de ativos de informação;
III. Monitoramento com sensores e câmeras;
IV. Proteção contra acesso visual externo;
V. Iluminação, temperatura, alimentação elétrica e umidade apropriada aos equipamentos que se encontram no ambiente;
VI. Mecanismos de prevenção de incêndios;
VII. Proteção contra ameaças físicas;
VIII. Iluminação de emergência;
IX. Contingência de energia, em caso de falha da fonte elétrica primária;
X. Controles de acesso físico.

§ 1º Os ativos de informação devem ser classificados, catalogados e identificados.

§ 2º Os ativos de informação devem possuir trava ou lacre de segurança que permita identificar qualquer tipo de violação física.

§ 3º Os *racks* utilizados para armazenamento de ativos de informação devem estar identificados e permanecer trancados.

Art. 11. O acesso físico ao Datacenter deve atender aos seguintes requisitos:

I. Somente ocorrerá mediante autorização da área responsável;
II. Quando autorizado, o responsável deverá identificar e registrar a pessoa, que será cadastrada no sistema de controle de acesso;
III. No caso de acesso para intervenções técnicas, deve ser precedido do preenchimento da Requisição de Mudança – RDM (modelo no Anexo B), que descreverá o motivo da intervenção, equipamentos, sistemas afetados e as pessoas envolvidas;
IV. Visitantes devem ser acompanhados por um integrante da área responsável e identificados em documento próprio contendo as seguintes informações:

a) Nome do visitante;
b) Matrícula ou CPF (no caso de não empregados);
c) Data e horário de entrada e saída;
d) Empresa;

e) Nome do responsável pela autorização do acesso;
f) Motivo do acesso;
g) Direitos concedidos de acessos aos ativos e às informações.

Art. 12. Compete ao DTI:

I. Assegurar o cumprimento dos requisitos de controle de acesso definidos no artigo anterior;
II. Administrar os mecanismos de controle de acesso;
III. Autorizar e controlar a entrada e saída de pessoas, mediante cadastramento e registro;
IV. Autorizar, controlar e registrar a entrada e a saída de equipamentos e ativos de informação.
V. Zelar pela restrição de acesso físico às informações;
VI. Salvaguardar os registros de acesso e assegurar sua integridade e disponibilidade durante 1 ano para efeito de auditorias futuras e, durante 5 anos, em casos de inconformidades;
VII. Identificar os ativos de informação;
VIII. Verificar mensalmente os registros de acesso e elaborar relatório com as inconformidades encontradas, se for o caso;
Manter a limpeza do ambiente, acompanhar e orientar o pessoal da limpeza.

Art. 13. A limpeza da sala-cofre e da sala de telecomunicação deve ser realizada por pessoas treinadas.

§ 1º Os horários da limpeza devem ser determinados com antecedência.

§ 2º A equipe responsável pela limpeza deve permanecer acompanhada por algum integrante da área responsável.

CAPÍTULO IV
DO ACESSO LÓGICO ÀS INFORMAÇÕES

Art. 14. O acesso aos sistemas de informações deve ser realizado de forma controlada e atender aos seguintes requisitos:

I. A concessão de acesso de um usuário ao sistema somente ocorrerá após devidamente autorizado pela autoridade competente;
II. A **autenticação** no sistema deve assegurar a identificação inequívoca do usuário por meio do uso de credencial de acesso;
III. Os acessos devem adotar a premissa de privilégio mínimo, necessário apenas para a realização das suas atividades funcionais;
IV. Os sistemas informatizados devem registrar os acessos de forma a permitir a identificação do gestor/colaborador e a rastreabilidade de suas ações.

Art. 15. O processo de autorização para concessão de acesso aos sistemas de informações deve observar os seguintes aspectos:

I. A concessão de acesso deve ser solicitada pela chefia do colaborador ou gestor de contrato à autoridade competente mediante o fornecimento de informações como justificativa, identificação completa do colaborador, níveis de acesso e período de acesso necessários;
II. A autoridade competente poderá delegar ao gestor do sistema a autorização das solicitações de concessão de acesso.

Art. 16. A concessão e exclusão de acesso aos sistemas de informações devem observar os seguintes aspectos:

I. Após autorizado pela autoridade competente, o acesso deve ser concedido pelo gestor do sistema mediante credenciamento do colaborador no sistema e fornecimento de sua credencial de acesso diretamente ao usuário;
II. O acesso deve ser concedido com a premissa de privilégio mínimo de acesso, necessários para a execução de suas atividades;
III. A validade da credencial de acesso deve obedecer ao previsto na autorização concedida, devendo sua renovação ser requerida em caso de necessidade;
IV. O colaborador deve assinar o Termo de Responsabilidade e Sigilo, que conterá as obrigações e responsabilidades no uso do sistema e no sigilo das informações;
V. O usuário deve receber instruções ou treinamento adequado para uso do sistema, como a troca de senha e operacionalização dos seus módulos, a fim de viabilizar o correto manuseio das informações e assegurar a sua integridade;
VI. A chefia ou gestor de contrato que solicitou o acesso deve informar a autoridade competente no caso em que o colaborador for desligado de suas funções, a fim de que sua credencial seja excluída do sistema.

Art. 17. O uso de credencial de acesso nos sistemas de informações deve atender aos seguintes requisitos:

I. Deve ser considerada de uso pessoal e intransferível e identificar unicamente o usuário;
II. No caso de credencial do tipo "usuário e senha", o sistema deve permitir a exigência no uso de senhas fortes (quantidade mínima de caracteres e uso de caracteres especiais) e a troca voluntária e obrigatória de senha;
III. No caso de credencial do tipo certificado digital, devem ser compatíveis com a ICP Brasil e/ou Autoridade Certificadora Interna do MPDFT.

Art. 18. Esta Portaria Normativa entrará em vigor na data de sua publicação, revogando-se as disposições em contrário.

Dê-se ciência, cumpra-se e publique-se.

ZENAIDE SOUTO MARTINS

ANEXO A - Modelo de Termo de Responsabilidade

MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____deste MPDFT, DECLARO, sob pena das sanções cabíveis nos termos da normas internas do MPDFT e da legislação aplicada que assumo a responsabilidade por:

I) tratar o(s) ativo(s) de informação como patrimônio do MPDFT;

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

III) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme as normas específicas do MPDFT;

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

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

Brasília, DF, _____de _____de _____ .

_____
ASSINATURA
Nome do usuário e seu setor organizacional

_____
ASSINATURA
Nome da autoridade responsável pela autorização do acesso

ANEXO B - Modelo de Requisição de Mudança

MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS

REQUISIÇÃO DE MUDANÇA – RDM

Departamento de Tecnologia da Informação – DTI

Objeto: Mudança do servidor web (S1234)

1. **Descrição da mudança**

2. **Justificativas**

3. **Escopo da Mudança**

   a. Ambientes impactados

   b. Itens de Configuração impactados e áreas responsáveis

ICs	Áreas

4. **Benefícios Esperados com a Mudança**

   a.

   b.

   c.

5. **Programação**

   a. Data e Hora da mudança

   b. Tempo estimado de execução

   c. Indisponibilidade prevista

6. **Atividades previstas**

   a. Antes da mudança:

Ação	Responsável	Data p/ conclusão	Status
1.			
2.			
3.			
4.			
5.			

   b. Durante a mudança:

Ação	Responsável	Data p/ conclusão	Status
1.			
2.			
3.			
4.			
5.			

   c. Depois da mudança:

Ação	Responsável	Data p/ conclusão	Status
1.			
2.			
3.			
4.			
5.			

7. **Ação de *Rollback* ou de Contingência**

8. **Equipe técnica responsável pela mudança**

Nome	Área	Telefone
1.		
2.		
3.		
4.		
5.		

9. **Coordenador da Mudança**

Publicado em 06 / 06 / 14

Aline Márcia de Oliveira Castro
Técnico Administrativo
MAT. 3275-1/MPDFT