PORTARIA N° 4.270/2019-MP/PGJ

A SUBPROCURADORA-GERAL DE JUSTIÇA, PARA A ÁREA JURÍDICO-INSTITUCIONAL, usando das atribuições que lhe foram delegadas pela Portaria nº 114/2018-MP/PGJ, de 12 de janeiro de 2018,

R E S O L V E :

CONCEDER aos membros abaixo discriminados licença para tratamento de saúde, com fulcro no art. 129 da Lei Complementar Estadual nº. 057, de 6/7/2006.

PROTOCOLO	NOME	PERÍODO
112175/2019	ANDRESSA ERICA AVILA PINHEIRO	01 a 05/07/2019
111657/2019	ARNALDO CELIO DA COSTA AZEVEDO	24 a 28/06/2019
111918/2019	DULCELINDA LOBATO PANTOJA	27/06 a 04/07/2019
111887/2019	EVANDRO DE AGUIAR RIBEIRO	24 a 26/06/2019
111886/2019	EVANDRO DE AGUIAR RIBEIRO	19/06/2019
113098/2019	GABRIELA RIOS MACHADO	15 a 16/07/2019
112237/2019	GUILHERME LIMA CARVALHO	01 a 15/07/2019
112224/2019	JANE CLEIDE SILVA SOUZA	01 a 25/07/2019
112899/2019	JOAO BATISTA DE ARAUJO CAVALEIRO DE MACEDO JUNIOR	08 a 12/07/2019
109901/2019	JULIANA CABRAL COUTINHO ANDRADE	15/05 a 13/07/2019
111643/2019	LAURO FRANCISCO DA SILVA FREITAS JUNIOR	08/07 a 06/08/2019
113085/2019	LIVIA TRIPAC MILEO CAMARA	15 a 19/07/2019
112349/2019	LIZETE DE LIMA NASCIMENTO	01 a 15/07/2019
112599/2019	LUZIANA BARATA DANTAS	03 a 05/07/2019
113007/2019	MARCOS ANTONIO FERREIRA DAS NEVES	11 a 15/07/2019
111782/2019	MARIA TERCIA AVILA BASTOS DOS SANTOS	24/06 a 23/07/2019
111692/2019	MYRNA GOUVEIA DOS SANTOS	22/06 a 05/07/2019
111802/2019	PAULA CAROLINE NUNES MACHADO	24/06/2019
111804/2019	PAULA CAROLINE NUNES MACHADO	25/06/2019
113066/2019	ROSANA PAES PINTO	15 a 29/07/2019
111728/2019	ROSANGELA ESTUMANO GONCALVES HARTMANN	26/06 a 25/07/2019

PUBLIQUE-SE, REGISTRE-SE E CUMPRA-SE.

GABINETE DA SUBPROCURADORIA-GERAL DE JUSTIÇA, PARA A ÁREA JURÍDICO-INSTITUCIONAL. Belém, 11 de junho de 2019.

CÂNDIDA DE JESUS RIBEIRO DO NASCIMENTO

Subprocuradora-Geral de Justiça,

área jurídico-institucional

PORTARIA N.° 4.271/2019-MP/PGJ

Institui e regulamenta a Política de Senhas de sistemas informatizados no Ministério Público do Estado do Pará

O PROCURADOR-GERAL DE JUSTIÇA DO MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ, no uso das atribuições conferidas pela Lei Complementar nº 57, de 06 de julho de 2006,

CONSIDERANDO a necessidade de estabelecer critérios relativos às senhas utilizadas nos sistemas informatizados, visando o incremento da segurança dos usuários e do ambiente computacional no âmbito do MPPA;

CONSIDERANDO a criticidade dos dados e informações que o Ministério Público do Estado do Pará dispõe em seus sistemas e bancos de dados;

CONSIDERANDO o significativo aumento de tentativas de acesso malicioso a sistemas informatizados deste Ministério Público;

CONSIDERANDO os relatórios sobre ataques cibernéticos no que tange à elevação de casos concretos de invasão de sistemas;

CONSIDERANDO a utilização massiva da metodologia "força bruta" para quebrar senhas de acesso;

CONSIDERANDO a Portaria 3008/2015-MP/PGJ, que institui a Política de Segurança da Informação do Ministério Público do Estado do Pará

CONSIDERANDO o Decreto nº 8.771, de 11 de maio de 2016, da Presidência da República, que Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações; e

CONSIDERANDO a norma internacional ISO/IEC 27002:2013, que trata de um código de prática para a gestão de segurança da Informação, incluindo um capítulo relativo a controle de acessos.

CONSIDERANDO a norma internacional ISO/IEC 27037:2012, que trata de Tecnologia da Informação – Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais.

RESOLVE:

CAPÍTULO I DAS DISPOSIÇÕES PRELIMINARES

Instituir a Política de Senhas para acesso a sistemas informatizados no âmbito do Ministério Público do Estado do Pará.

CAPÍTULO II DOS CONCEITOS

Considera-se, para fins desta Portaria Normativa:

1. Acesso: Estabelecimento de conexão entre um indivíduo ou unidade e um sistema de comunicação ou de informações. A partir do Acesso podem ocorrer a transferência de dados e a ativação de processos computacionais;
2. Ataque: Ato de tentar desviar dos controles de segurança de um programa, sistema ou rede de computadores. Um ataque pode ser ativo, tendo por resultado a alteração dos dados; ou passivo, tendo por resultado a liberação dos dados. O fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia de contramedidas existentes;

Autenticidade: Qualidade de um documento ser o que diz ser, independente de se tratar de minuta, original ou cópia e que é livre de adulterações ou qualquer outro tipo de corrupção;

1. Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
2. Conta: Permissão para acesso a um serviço. A permissão é obtida após o registro de dados específicos do usuário, no servidor, que definem o ambiente de trabalho desse usuário. O registro pode incluir configurações de tela, configurações de aplicativos e conexões de rede. O que o usuário vê na tela, além de quais arquivos, aplicativos e diretórios ele tem acesso é determinado pela maneira com que foi configurada a conta do usuário. Esta conta é una, indivisível, de uso pessoal e restrito, não podendo, em nenhuma hipótese, ser compartilhada ou repassada a qualquer pessoa;
3. Controle de Acesso: Conjunto de componentes dedicados a proteger a rede, aplicações Web e instalações físicas contra o acesso não autorizado, permitindo que somente organizações ou indivíduos previamente identificados e autorizados possam utilizá-las. Restrições ao acesso às informações de um sistema, exercidas pela gerência de segurança da entidade detentora daquele sistema;

Controles: Práticas, procedimentos e mecanismos utilizados para a proteção da informação e dos ativos a ela correlacionados, que podem ser de natureza administrativa, técnica, legal ou de gestão;

Criptografia: Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, sendo usada para autenticar a identidade de um usuário, autenticar transações, proteger a integridade de transferências e proteger o sigilo de comunicações pessoais e corporativas;

1. Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las;
2. Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;
3. Recursos: Patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos das entidades, tanto os produzidos internamente quanto os adquiridos pelo MPPA;

Senhas Administrativas: senhas que permitem que determinados usuários acessem equipamentos e sistemas que compõem a infraestrutura computacional do Ministério Público com privilégios administrativos;

Senhas institucionais: Senhas não utilizadas de forma individual, como senhas de e-mail de Promotorias de Justiça localizadas no interior do Estado ou senhas de e-mail de setores específicos do Ministério Público.

Single sign-on: senha única para acesso a diversos recursos, não havendo possibilidade de criação de senhas distintas para uso em sistemas ou ferramentas que adotem esta técnica.

As disposições desta Portaria se aplicam a todos os usuários que façam uso dos recursos de Tecnologia da Informação do MPPA.

CAPÍTULO III Das Senhas

Da Utilização das Senhas

Membros, Servidores e Estagiários do MPPA, na ativa e no efetivo exercício de suas atribuições, possuem, cada um, uma senha de uso de acesso individual, pessoal e intransferível aos recursos de tecnologia do Ministério Público.

1.O usuário é responsável por manter sob sigilo sua senha de acesso.

2.O usuário é responsável cível, administrativa e criminalmente por qualquer ação realizada que utilize sua senha de acesso no ambiente computacional do MPPA, cabendo medidas em caso de irregularidades detectadas.

A política de acesso a determinado recurso tecnológico, mediante uso de senhas ou não, será definida pelo Comitê Estratégico de Tecnologia da Informação do Ministério Público.

Não é permitido tentar obter ou conseguir acesso não autorizado a qualquer recurso de tecnologia da Informação do Ministério Público, podendo ser adotadas medidas cabíveis contra o servidor responsável.

Quando o usuário for desligado do Ministério Público, sua senha de acesso será cancelada tão logo o Departamento de Informática for cientificado do desligamento.

Seção II

Da Complexidade das Senhas

As senhas de acesso devem atender aos seguintes parâmetros de complexidade, visando dificultar possíveis ataques:

1. Devem conter, no mínimo, 10 caracteres.
2. Deve conter, no mínimo, 1 caractere de cada um dos grupos abaixo:
3. Letras maiúsculas;
4. Letras minúsculas;
5. Números.
6. Caracteres não alfanuméricos, como, por exemplo, ponto de exclamação (!), cifrão ($), porcentagem (%) ou sinal numérico (#)

Devem ser isentas de caracteres idênticos consecutivos:

1. Devem ser isentas de sequências numéricas ou alfabéticas com 4 ou mais caracteres.

É importante que todas as senhas atendam às boas práticas de segurança da informação, tais como:

1. Não devem conter, em todo ou parte, nome do usuário ou sua matrícula institucional.
2. Não devem conter datas, como datas de aniversário, data de admissão, etc.

Não devem conter informações pessoais de nenhuma espécie.

1. Não devem conter informações de fácil dedução.

Parágrafo único: Senhas geradas automaticamente por sistemas informatizados devem utilizar a maior complexidade possível no referido sistema, em relação a quantidade de caracteres e presença de outros grupos de caracteres, como símbolos, letras acentuadas ou sinais de pontuação.