TEXTO INTEGRAL

ATO NORMATIVO 27/2020

ATO NORMATIVO TJ N.º 27/ 2020

Estabelece as normas para Gestão de Acesso a Recursos de Tecnologia da Informação e Comunicação do Tribunal de Justiça do Estado do Rio de Janeiro e dá outras providências.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO, Desembargador Claudio de Mello Tavares, no uso de suas atribuições legais;

CONSIDERANDO o que dispõe a Lei Federal n.º 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;

CONSIDERANDO o que dispõe a Lei Federal n.º 13.709, de 14 de agosto de 2018, com a redação dada pela Lei Federal n.º 13.853, de 08 de julho de 2019, sobre a proteção de dados pessoais, que altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

CONSIDERANDO o que dispõe a Resolução n.º 176/2013 e suas alterações, do Conselho Nacional de Justiça, de 10 de junho de 2013, que institui o Sistema Nacional de Segurança do Poder Judiciário;

CONSIDERANDO o que dispõe a Resolução n.º 211/2015 do Conselho Nacional de Justiça - CNJ, de 15 de dezembro de 2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC JUD);

CONSIDERANDO o que dispõe a Resolução n.º 215/2015 do Conselho Nacional de Justiça - CNJ, de 16 de dezembro de 2015 que estabeleceu as regras sobre o acesso à informação, no âmbito do Poder Judiciário;

CONSIDERANDO o que dispõe a Resolução TJ/OE n.º 09/2017, de 07 de agosto de 2017, aprovada na sessão administrativa do Órgão Especial do dia 07 de agosto de 2017 (Processo Administrativo n.º 2016 000230);

CONSIDERANDO o que dispõe a Resolução TJ/OE n.º 05/2019, de 27 de fevereiro de 2019, sobre a política de segurança da informação, aprovada na sessão administrativa do Órgão Especial do dia 25 de fevereiro de 2019 (Processo Administrativo n.º 2018-107905);

CONSIDERANDO o que dispõe a Portaria da Secretaria Geral do Conselho Nacional de Justiça n.º 47/2017 que instituiu a Política de Segurança da Informação do CNJ;

CONSIDERANDO o que dispõe o Ato Normativo TJ n.º 08/2018, de 22 de maio de 2018, sobre o Serviço de Informação ao Cidadão, do Acesso as Informações do Poder Judiciário do Estado do Rio de Janeiro;

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1º. A gestão de acesso físico e eletrônico às informações sob o controle do Poder Judiciário do Estado do Rio de Janeiro (PJERJ) será disciplinada pelo presente Ato Normativo.

Art. 2º. O acesso à informação sob o domínio do PJERJ seguirá o princípio do privilégio mínimo, ou seja, somente serão concedidas permissões imprescindíveis e suficientes, pelo tempo necessário, para que o usuário possa realizar suas atividades.

Art. 3º. Cabe aos responsáveis pelos recursos de Tecnologia da Informação e Comunicação (TIC) zelar pela sua segurança, garantindo que somente pessoas autorizadas tenham acesso.

Art. 4º. O PJERJ deverá realizar as ações necessárias para o atendimento da Lei Federal n.º 13.709, de 14 de agosto de 2018, com a redação dada pela Lei Federal n.º 13.853, de 08 de julho de 2019, para a proteção de dados pessoais dos usuários garantindo o uso destas apenas para as atividades finalistas as quais os dados estão vinculados.

§ 1º. Cabe aos usuários internos do PJERJ que utilizam dados e informações em meio físico garantir o seu correto uso, evitando que possam ser utilizados para outros fins.

§ 2º. Cabe à Diretoria Geral de Tecnologia da Informação e Comunicação de Dados (DGTEC) garantir que os dados e informações armazenados nas bases corporativas sejam protegidos, evitando que possam ser desviados e utilizados para atividades diversas ao seu objetivo.

CAPÍTULO II
DA GESTÃO DE ACESSO FÍSICO

Art. 5º. Cabe à Diretoria Geral de Segurança Institucional (DGSEI) a gestão do acesso físico a todas as instalações do PJERJ, de forma a impedir que dados e informações possam ser acessadas indevidamente.

Parágrafo único. Complementarmente, os responsáveis e funcionários de cada unidade do PJERJ devem zelar para que não haja acesso físico indevido a dados e informações em suas respectivas unidades.

Art. 6º. A violação de qualquer instalação, local físico ou ativo de TIC do PJERJ deve ser comunicada imediatamente à DGSEI, através dos canais competentes.

Art. 7º. As áreas de acesso restrito devem estar devidamente fechadas e sempre que possível monitoradas por câmeras de vigilância, sob o controle da DGSEI.

Art. 8º. Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos eletrônicos.

Art. 9º. Os documentos impressos devem ser protegidos contra perda, reprodução e uso não autorizado.

§ 1º. Os documentos impressos em impressoras departamentais ou compartilhadas devem ser recolhidos imediatamente.

§ 2º. A impressão de documentos sigilosos deverá ser realizada sob supervisão do responsável.

Art. 10. Visando à proteção das informações em meio físico, cabe ao usuário trabalhar adotando o princípio da mesa limpa, não deixando processos ou quaisquer documentos expostos quando se ausentar do local.

Art. 11. O acesso físico ao Data Center deverá ser feito por sistema forte de autenticação, mediante uso de solução de TIC própria.

Parágrafo único. O acesso físico por meio de chave apenas poderá ocorrer em situações de emergências, quando a segurança física do Data Center estiver comprometida, seja por motivo de incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

Art. 12. A relação de pessoas autorizadas a acessar fisicamente o Data Center deverá ser atualizada imediatamente, pelo Diretor da área de infraestrutura de TIC da DGTEC, em casos de alterações, como admissões, impedimentos ou desligamentos, e as atualizações deverão ser implementadas de imediato, nos sistemas de controle de acesso.

Art. 13. O acesso físico eventual de visitantes ao Data Center será sempre registrado, acompanhado e supervisionado por funcionário especificamente designado pelo responsável pelo Data Center, e ocorrerá mediante declaração de responsabilidade e sigilo assinada pelo visitante em documento próprio, sem prescindir da prévia autorização do Diretor da área de infraestrutura de TIC da DGTEC.

Art. 14. O Data Center onde se localizam os ativos de infraestrutura de TIC deverá ter tratamento diferenciado com os seguintes requisitos:

I. acesso somente de pessoas credenciadas e previamente autorizadas;

II. o acesso à sala obrigatoriamente dar-se-á por sistema biométrico e registro do acesso em relatório de entrada dos usuários;

III. monitoramento pleno do ambiente interno por intermédio de câmeras de vigilância de Circuito Fechado de Televisão (CFTV);

IV. sistema de detecção de incêndio especial, independentemente de se apresentarem inodoras e invisíveis.

V. ramal telefônico especial, para acionamento em caso de emergência, interligado com o Centro Integrado de Segurança do Poder Judiciário (CISPJ);

VI. instalação de sistema de monitoramento com câmeras, interligado com o CISPJ.

CAPÍTULO III
DA GESTÃO DE ACESSO A RECURSOS DE TIC

Art. 15. Para efeitos deste Ato Normativo, ficam estabelecidas as seguintes definições:

I. nome de usuário, também chamado "login", é a conta de acesso atribuída individualmente a um usuário para acesso aos recursos de TIC;

II. usuários internos: magistrados e servidores do PJERJ, bem como outros a que se reconhecer acesso às funcionalidades internas do sistema de processamento em meio eletrônico, tais como: estagiários, conciliadores, juízes leigos colaboradores, prestadores de serviço e visitantes, dentre outros;

III. usuários externos: todos os demais usuários, incluídos partes, advogados, membros do Ministério Público, defensores públicos, peritos e leiloeiros;

IV. certificado digital: é um arquivo eletrônico que funciona como uma assinatura digital, que garante proteção às transações eletrônicas.

Art. 16. Os certificados digitais do domínio do PJERJ pertencem obrigatoriamente à cadeia "AC JUS" e podem ser emitidos para: pessoa jurídica (institucional) e pessoas físicas (usuários internos).

§ 1º. Os cerificados digitais emitidos para servidores de TIC (equipamentos de TIC de processamento de sistemas informatizados), do tipo SSL (Secure Sockets Layer), poderão ser emitidos fora da cadeia "AC JUS".

§ 2º. Os certificados digitais são pessoais e intransferíveis independente do meio no qual esteja instalado, cabendo a seu titular a guarda do arquivo ou dispositivo, bem como a proteção do login e da senha.

Art. 17. Cada usuário interno pessoa física, que no uso de suas atribuições precisar de assinatura digital, só terá direito a um certificado digital armazenado em token ou smartcard e outro armazenado num único desktop e notebook de uso corporativo.

Parágrafo único. Os Magistrados farão jus a 02 (dois) certificados digitais.

Art. 18. Cabe à DGTEC elaborar, e após apreciação do Comitê Gestor de Segurança da informação (CGSI) e aprovação do Presidente do PJERJ, implementar e divulgar políticas e boas práticas na utilização de senhas, visando prevenir o acesso de usuários não autorizados aos sistemas de informação.

SEÇÃO I
DA IDENTIFICAÇÃO DO USUÁRIO (LOGIN) E SENHA DE ACESSO

Art. 19. O acesso a recursos de TIC tais como rede, sistemas corporativos e outros está condicionado a identificação e autenticação da conta do usuário através de um único login ou certificado digital e senha, e outros fatores de autenticação, conforme as necessidades de cada ativo de TIC.

Art. 20. O login e respectiva senha serão únicos e atribuídos a cada usuário, de forma individual e intransferível, de uso exclusivo do seu titular, não podendo ser compartilhado com outros usuários.

§ 1º. É vedado, a qualquer usuário, se apropriar e compartilhar login e senha pertencente a outro usuário.

§ 2º. Os usuários são responsáveis por todos os acessos e atividades desenvolvidas através do seu login, podendo ser responsabilizados pelos danos decorrentes de sua má utilização.

§ 3º. Caso seja detectado acesso ou atividade suspeita, o login do usuário será desabilitado podendo ensejar a instauração de processo administrativo disciplinar.

Art. 21. A solicitação de login deverá ser feita à DGTEC, através de seus canais de atendimento.

Parágrafo único. Os Usuários deverão fornecer todos os dados necessários para a sua identificação.

Art. 22. Um login só poderá ser criado nos seguintes casos:

I. usuário interno: se estiver cadastrado em uma das bases de dados de gestão de pessoas do PJERJ;

II. usuário externo: se estiver cadastrado na base de dados de usuários externos, no cadastro presencial do PJERJ ou possuir certificado digital ICP Brasil.

§ 1º. A DGTEC manterá integração do sistema de controle de acesso com as bases de dados de gestão de pessoas a fim de garantir a correta identificação dos usuários e a segurança dos sistemas corporativos.

§ 2º. Não será permitido o cadastro de contas de correio eletrônico genéricas (ex.: contato@...; vendas@...) para usuários externos pessoas físicas.

§ 3º. Não será permitida a concessão de login genérico para qualquer usuário.

Art. 23. Caso o usuário não esteja em uma das bases de dados de gestão de pessoas ou no cadastro presencial, deverá solicitar o respectivo cadastramento ao órgão responsável pela gestão da base de dados vinculada ao seu perfil, para posteriormente solicitar o login.

Art. 24. A criação de logins para os usuários internos do PJERJ obedecerá ao padrão estabelecido pela Instrução Normativa CNJ n.º 51/2013, no seguinte formato: "prenome.sobrenome".

§ 1º. Deverá ser utilizado preferencialmente o sobrenome extraído da filiação do usuário para a composição do login previsto no caput deste artigo.

§ 2º. Os pedidos de troca de login deverão ser devidamente justificados e submetidos obrigatoriamente à Administração Superior, através de processo administrativo.

§ 3º. O padrão estabelecido no caput deste artigo será aplicado aos logins que forem criados a partir da publicação deste ato normativo.

Art. 25. Os logins de usuários internos referentes aos certificados digitais de pessoas físicas armazenados no servidor de rede do PJERJ, por definição da ferramenta será o número do CPF.

Art. 26. O usuário externo terá como login o número do CPF, para acesso aos sistemas corporativos, sem acesso a recursos da rede informatizada do PJERJ.

Art. 27. Todo login será vinculado a um perfil limitado as atividades realizadas pelos usuários, conforme art. 2º deste Ato Normativo.

Art. 28. É de responsabilidade exclusiva do usuário a manutenção do sigilo de sua senha de acesso aos ativos de TIC do PJERJ.

SECÃO II
DA SENHA DE USUÁRIOS

Art. 29. Recomenda-se que as senhas de identificação tenham tamanho mínimo de 8 (oito) caracteres e atendam, no mínimo, 3 (três) dos requisitos abaixo:

I. pelo menos uma letra maiúscula;

II. pelo menos uma letra minúscula;

III. pelo menos um número;

IV. pelo menos um caractere especial.

§ 1º. Recomenda-se que não se utilizem as 3 (três) últimas senhas estabelecidas pelo usuário, quando do procedimento de alteração, exceto se houver violação ou vazamento da senha.

§ 2º. Os usuários deverão trocar suas senhas obrigatoriamente após o período de 180 (cento e oitenta) dias.

§ 3º. A DGTEC poderá excepcionalmente propor alteração der prazos para troca de senha, visando adequar as características de acesso de novas atividades ou funcionalidades, com apreciação pelo CGSI e aprovação do Presidente do PJERJ.

SEÇÃO III
DA INATIVAÇÃO DO USUÁRIOS

Art. 30. O usuário interno terá seu login desabilitado, por questões de segurança, nas seguintes situações:

I. se ficar mais de 95 (noventa e cinco) dias sem acessar qualquer sistema corporativo (ou rede);

II. se passar definitivamente para inatividade e ficar mais de 180 (cento e oitenta) dias sem acessar qualquer sistema corporativo;

III. se for desligado definitivamente ou perder o vínculo com o PJERJ;

IV. se errar a senha 5 (cinco) vezes consecutivas ou alternadamente no mesmo dia;

V. caso seja identificado o vazamento ou a descoberta da senha por terceiros, ou haja fortes indícios de que isso tenha acontecido.

§ 1º. Não estão incluídos na regra estabelecida nos incisos I, II e III deste artigo, os usuários que possuam cadastros que não derivem diretamente do vínculo com o PJERJ para acessar processos judiciais, pelo cadastro presencial e sejam partes de processos judiciais ativos.

§ 2º. A reabilitação do login poderá ser solicitada à DGTEC diretamente pelo usuário, a qualquer tempo, pelos canais de atendimento, justificando o motivo se necessário, salvo na situação prevista no inciso III deste artigo.

§ 3º. Os usuários internos terceirizados e visitantes deverão ter suas contas configuradas, sempre que possível, para expirar e serem bloqueadas automaticamente pelos sistemas de informação ao término de seus projetos ou período de prestação de serviço ou permanência do PJERJ.

§ 4º. É dever do fiscal do contrato ou responsável pelo visitante comunicar à DGTEC, via abertura de chamado, caso o usuário descrito no parágrafo anterior pare de prestar serviços para o PJERJ antes do período previsto para expiração do acesso.

§ 5º. Enquanto a área responsável não notificar a DGTEC o desligamento prestador de serviço, o acesso será mantido e as responsabilidades atribuídas para o usuário em questão, permanecerão com a área responsável pelo contrato ou visitante.

Art. 31. O usuário externo que ficar mais de 180 (cento e oitenta) dias sem acessar o sistema para o qual está cadastrado será desabilitado, exceto se estiver cadastrado para acessar processos judiciais pelo cadastro presencial e sejam partes de processos judiciais ativos.

SEÇÃO IV
REATIVAÇÃO DE LOGIN

Art. 32. Os usuários que forem inativados deverão solicitar a reativação de seu login pelos canais de atendimento da DGTEC.

Parágrafo único. No caso previsto no inciso V, do art. 30, deste Ato Normativo o usuário será orientado a trocar sua senha obrigatoriamente, independente da regra de temporalidade.

SEÇÃO V
DA CONCESSÃO DE ACESSOS AOS RECURSOS DE TIC

Art. 33. Após a criação do login, a concessão a qualquer recurso de TIC deverá ser solicitada pelos canais de atendimento da DGTEC, com informação do autorizador (superior hierárquico), no caso de usuário interno, para o exclusivo exercício das atividades a qual o usuário foi designado.

§ 1º. A inclusão, alteração ou exclusão de acessos aos recursos de TIC para usuários internos do PJERJ deverá ser comunicada e solicitada pelo seu superior hierárquico imediato.

§ 2º. Para usuários externos vinculados a outros órgãos públicos, o acesso deverá ser requisitado pelo chefe do órgão.

§ 3º. No caso de usuários externos não vinculados a órgãos públicos, tais como partes processuais ou advogados, o pedido de inclusão, alteração ou exclusão deverá ser feito pelo próprio.

§ 4º. Só serão concedidas as permissões de acesso a recursos de TIC que sejam necessárias para o cumprimento das atribuições do usuário.

Art. 34. Além de cumprirem os requisitos insculpidos neste Ato Normativo, os prestadores de serviços que acessarem recursos de TIC também deverão assinar o termo de confidencialidade e sigilo, abarcando os limites de uso, bem como ciência quanto responsabilidade em caso de má utilização dos recursos de TIC do PJERJ, sem o qual não poderão ser cadastrados na respectiva base de dados de gestão de pessoas.

Art. 35. Os usuários internos do PJERJ não poderão se conectar a mais de um recurso de TIC fixo, simultaneamente com o seu login.

§ 1º. A regra estabelecida no caput deste artigo não se aplica a dispositivos móveis cadastrados na conta de cada usuário.

§ 2º. O funcionários e colaboradores da área de TIC, por dever de ofício, também não se enquadram nas restrições estabelecidas neste artigo.

Art. 36. A necessidade de uso de recursos TIC da rede corporativa por outros órgãos públicos ou privados será individualmente analisada pela DGTEC, com apreciação pelo CGSI, que submeterá a deliberação ao Presidente do PJERJ, a quem competirá autorizar.

SEÇÃO VI
DO ACESSO AO PROCESSO ELETRÔNICO

Art. 37. Em se tratando de processos eletrônicos, a prática de atos processuais e a consulta aos autos do processo no sítio do PJERJ deverão ser realizadas através de login e senha e certificado digital ICP Brasil nos atos assim estabelecidos em legislação própria.

Parágrafo Único. A consulta processual completa permite a visualização de todos os andamentos processuais, os documentos e arquivos a eles anexados; enquanto que a consulta pública permite apenas a visualização dos andamentos processuais.

Art. 38. Alternativamente a prática de atos processuais e a consulta aos autos do processo no sítio do PJERJ poderão ser feitas sem certificado digital desde que precedidas de Cadastro Presencial.

Art. 39. O Cadastro Presencial deverá ser feito pelo usuário interessado em atuar em processo eletrônico, nos órgãos ou serventias eletrônicas, mediante assinatura do termo de cadastramento e adesão ao sistema, com a apresentação compulsória dos documentos originais acompanhados de cópia, conforme estabelecido em legislação própria.

Parágrafo único. O cadastro presencial será igualmente obrigatório para os casos em que for necessário o acesso, via internet, à movimentação de processos que tramitem em segredo de Justiça e para acesso às audiências gravadas no sistema de registro audiovisual.

Art. 40. Todos os serventuários, terceirizados, estagiários ou funcionários cedidos, que atuarem em processo eletrônico, de qualquer esfera ou instância do Tribunal de Justiça, deverão utilizar também a assinatura eletrônica ou identificação, através do cadastro presencial, que será disponibilizado na serventia em que esteja lotado, em aplicativo próprio a ser gerenciado pelo responsável pela serventia.

§ 1º. Os serventuários que utilizarem o cadastro presencial estarão dispensados de apresentação dos documentos mencionados nos incisos I e II do artigo anterior, por já terem seus dados arquivados na Diretoria Geral de Gestão de Pessoas (DGPES), mas deverão obrigatoriamente exibir um documento funcional com foto que o identifique, no momento da realização do cadastro.

§ 2º. O serventuário, terceirizado, estagiário, bem como o funcionário cedido, que já estejam cadastrados, utilizarão o mesmo login e senha utilizado nos demais sistemas corporativos do PJERJ.

Art. 41. O PJERJ poderá estabelecer convênios com outros órgãos com a finalidade de facilitar o cadastramento e/ou compartilhar o cadastro presencial, de acordo com o estabelecido na Lei nº. 11.419 de 19 de dezembro de 2006.

SEÇÃO VII
DA PERDA DE ACESSOS POR MUDANÇA DE LOTAÇÃO

Art. 42. O usuário interno que mudar de lotação perderá o acesso aos sistemas corporativos e aos ativos de rede referentes as atividades da sua última lotação, exceto aos sistemas de uso pessoal e em caso de acumulo de funções ou atribuições, devidamente autorizados.

§ 1º. Magistrados e seus assessores que exercerem suas atividades em mais de uma lotação não se enquadram na regra do caput deste artigo.

§ 2º. Somente o novo superior hierárquico do usuário poderá autorizar a DGTEC a conceder as permissões de acesso aos sistemas corporativos e ativos de rede vinculados à unidade.

§ 3º. Estão incluídos na regra estabelecida no caput deste artigo os funcionários e magistrados que passarem à inatividade (aposentadoria) ou disponibilidade (para outros órgãos públicos).

SEÇÃO VIII
DO ACESSO AO CORREIO ELETRÔNICO (e mail)

Art. 43. Compete à DGTEC definir, revisar e atualizar regras, elaborar e divulgar políticas e manuais de melhores práticas na utilização do correio eletrônico, com apreciação pelo CGSI e aprovação do Presidente do PJERJ, a fim de reduzir os riscos gerados na utilização deste meio de comunicação.

Art. 44. A caixa postal (conta) de correio eletrônico, que poderá ser individual ou compartilhada, será disponibilizada somente aos usuários ou órgãos previamente autorizados.

Art. 45. Fica definido como padrão de contas dos usuários e dos endereços de correio eletrônico o formato prenome.sobrenome@tjrj.jus.br, mantidos os endereços eletrônicos existentes até a publicação deste ato normativo.

Art. 46. Podem ser criadas caixas postais institucionais e listas de distribuição internas de correio eletrônico, a pedido dos titulares das unidades.

Parágrafo único. Adota se como padrão para as listas de distribuição o formato nome1.nome2@tjrj.jus.br.

Art. 47. As caixas postais de correio eletrônico são de propriedade do PJERJ, passíveis de monitoração pela DGTEC em caso de fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas ou serviços, com a prévia autorização do chefe imediato, do CGSI, ou do Presidente do PJERJ.

Parágrafo único. Tratando se de correio eletrônico cujo usuário seja magistrado, eventual monitoramento pela DGTEC só pode ocorrer com prévia apreciação do CGSI, e aprovação do Presidente do PJERJ, e com aviso imediato ao usuário por qualquer meio de comunicação pessoal.

Art. 48. É vedado o envio, replicação ou encaminhamento de mensagens, por meio do correio eletrônico, de conteúdo não relacionado às atividades precípuas do PJERJ.

§ 1º. Só será permitido o uso do correio eletrônico para veiculação de campanhas internas, de caráter social, mensagens informativas ou outras que eventualmente possam ter conteúdo vedado, mediante autorização do Presidente do PJERJ.

§ 2º. O usuário deverá informar imediatamente ao remetente o recebimento de mensagens encaminhadas por equívoco, devido a endereçamento incorreto, excluindo a imediatamente.

Art. 49. É vedado a utilização e o cadastramento de conta de correio eletrônico de domínio do PJERJ em formulários ou sítios eletrônicos não relacionados ao trabalho.

Art. 50. É vedado a alteração de layout, adulteração da logomarca, inclusão de imagens ou logomarcas de terceiros, nas contas de correio eletrônico enviadas de caixas postais eletrônicas institucionais ou individuais do PJERJ.

Art. 51. Caso o usuário precise cadastrar o seu endereço eletrônico institucional em site relacionado ao trabalho, não deverá, em hipótese alguma, reproduzir a senha institucional neste.

Art. 52. A fim de reduzir o problema com spam, é vedado o cadastramento de conta de correio eletrônico corporativa em formulários de empresas e/ou sites de relacionamento, compras, anúncios ou qualquer outro que solicite o preenchimento de um endereço eletrônico.

Art. 53. Caberá ao Presidente do PJERJ autorizar a liberação de listas de distribuição de contas de correio eletrônico para órgãos e usuários do PJERJ.

Parágrafo único. Recomenda se que o encaminhamento de mensagens eletrônicas para vários destinatários, de forma simultânea, seja feito por meio das listas ou do campo cópia oculta.

Art. 54. O envio de mensagem de correio eletrônico automática por aplicações através do servidor relay deverá ser registrado para autorização do setor competente da DGTEC.

Parágrafo único. Os desenvolvedores não poderão criar nenhuma conta de correio eletrônico fora dos padrões adotados pelo PJERJ, devendo ser feita uma solicitação ao setor de contas de correio eletrônico para sua criação e registro, ressalvada a manutenção dos endereços eletrônicos existentes na data de publicação desta resolução.

Art. 55. Caberá a cada usuário a gestão de sua caixa de correio eletrônico, incumbindo lhe que zele para que esta não exceda os limites de armazenamento estabelecidos.

Art. 56. Por questões de segurança, os arquivos anexados em mensagens recebidas poderão ser bloqueados, por possivelmente conterem softwares maliciosos ou conduzirem à sites maliciosos.

Parágrafo único. A DGTEC manterá uma lista de tipos de arquivos bloqueados poderá ser consultada na página da Intranet do PJERJ.

Art. 57. Por questão de segurança, recomenda se ao usuário não abrir mensagens de remetente ou conteúdo suspeito.

Parágrafo único. Em caso de dúvida, deverá o usuário solicitar suporte à DGTEC por meio da abertura de solicitação de serviço, junto aos canais de atendimento.

Art. 58. O recebimento de mensagens será filtrado para bloqueio de mensagens que contenham finalidades comerciais (spam), boatos maliciosos (hoaxes) e, ainda, outras hipóteses funcionalmente indesejáveis.

SEÇÃO VIII
DO ACESSO À INTERNET

Art. 59. O acesso dos usuários da rede corporativa à Internet deve ser feito exclusivamente por meio da única ligação existente entre o PJERJ e a rede mundial.

Art. 60. O acesso à internet através da rede corporativa é permitido somente aos usuários previamente autorizados, através de login e senha.

Art. 61. Os acessos à internet são passíveis de identificação quanto a login, endereço da máquina do usuário e site acessado.

Art. 62. Conexões com a internet, através de linha discada e/ou modem, somente poderão ser adotadas nas estações não interligadas à rede corporativa do PJERJ, enquanto permanecerem totalmente isoladas e com autorização da DGTEC.

Art. 63. É vedada a conexão e ou acesso à internet disponibilizada por terceiros, dentro ou fora das dependências do PJERJ.

Art. 64. A detecção de ligações independentes entre a internet e o Tribunal de Justiça, Fórum Central, Fóruns Regionais, Comarcas, Juizados Especiais e demais Órgãos do PJERJ, implicará na desconexão imediata da estação, até a apuração de responsabilidades e adoção das providências cabíveis.

Art. 65. É vedado o acesso a sites da internet de conteúdo não autorizado, dentre as categorias padronizadas bloqueadas pelas soluções de segurança de borda, como por exemplo de conteúdo:

I. incentivo ao alcoolismo;

II. utilitários anônimos;

III. blogs/wiki;

IV. exploits;

V. chats;

VI. namoro/encontros;

VII. qualquer tipo de descriminação;

VIII. drogas;

IX. apologia à drogas;

X. violência;

XI. jogos;

XII. bebidas;

XIII. nudez;

XIV. mensagem Instantânea;

XV. download de mídia;

XVI. compartilhamento de mídia;

XVII. compartilhamento de arquivo;

XVIII. repositório de rede pessoal;

XIX. páginas pessoais;

XX. phishing;

XXI. pornografia;

XXII. atividade potencialmente criminal;

XXIII. hacker;

XXIV. software ilegal;

XXV. profanação;

XXVI. controle remoto;

XXVII. conteúdo sexual;

XXVIII. redes sociais;

XXIX. urls de spam;

XXX. spyware/adware/keyloggers;

XXXI. streaming media;

XXXII. fumo/tabaco;

XXXIII. apologia ao crime;

XXXIV. armas;

XXXV. webmail;

XXXVI. encontro virtual;

XXXVII. telefonia IP (VOIP).

§ 1º. A vedação disposta no caput deste artigo é extensiva a webmail de provedores externos a rede corporativa do PJERJ.

§ 2º. Comprovada a imperiosa necessidade de serviço, o acesso poderá ser concedido temporariamente pela DGTEC, após apreciação pelo CGSI e autorização do Presidente do PJERJ, mediante solicitação por escrito, assinada pelo chefe imediato do órgão no qual o usuário está lotado.

§ 3º. A DGTEC poderá, sem prévio aviso, bloquear o acesso a sites que potencialmente ameacem a segurança da rede corporativa do PJERJ

Art. 66. É vedada a utilização de softwares de mensagens instantâneas e voz sobre IP (VoIP) não homologados e autorizados pela DGTEC.

SEÇÃO IX
DA GESTÃO DE ACESSO A INFRAESTRUTURA DE TIC

Art. 67. A DGTEC deverá adotar sistema de gestão de identidades por meio do qual será gerida à concessão de credenciais de acesso aos recursos de infraestrutura de TIC de sua administração, que desempenhe as funções de autenticação e autorização, com deliberação pelo CGSI e aprovação pelo Presidente do PJERJ, cujos objetivos serão:

I. identificar usuário;

II. eliminar a necessidade de uso de contas genéricas, de usuário final com perfil especial ou de administrador;

III. autorizar o acesso somente aos recursos necessários, observando se a regra de privilégio mínimo.

§ 1º. Mediante justificativa tecnicamente fundamentada, a área responsável pelo processamento de dados poderá conceder o acesso à conta de acesso privilegiado ou administrador para execução de atividade temporária e especial.

§ 2º. O sistema de que trata o caput deste artigo deverá atender, ao menos, os seguintes requisitos:

I. cadastramento de informações do usuário;

II. suportar acesso baseado em papeis ou "Role Based Access" (RBAC);

III. definir diferentes níveis de privilégio de acesso para um usuário;

IV. vincular um usuário a um ou mais papeis;

V. possuir interface gráfica de gerenciamento;

VI. suportar protocolos seguros de comunicação para transporte de dados de autenticação;

VII. gerir os acessos conforme seu ciclo de vida: ativo, inativo, revogado e cancelado.

Art. 68. As ações praticadas por usuários deverão ser registradas em servidor de registro de eventos (logs), para auditoria posterior, de modo que seja possível identificar preferencialmente:

I. quem executou determinada ação;

II. quais ações foram executadas;

III. quando as ações foram executadas;

IV. em qual ativo de informação as ações foram executadas.

Art. 69. Os eventos armazenados em logs poderão ser definidos conforme a necessidade de informação que deverá ser disponibilizada em casos de auditoria, requerimento da Corregedoria Geral da Justiça (CGJ) no âmbito de sua competência, investigação de ações, problemas ou para detecção de condutas que configurem mau uso dos recursos de TIC.

§ 1º. Por mau uso entendem se as ações, propositais ou não, que configurem ataques de reconhecimento, força bruta, negação de serviço, estouro de buffer, engenharia social, phishing, exploração de vulnerabilidade, pós exploração de vulnerabilidade dentre outras condutas de natureza similar que sejam praticadas contra os ativos de informação do PJERJ.

§ 2º. O tempo de retenção desses logs deverá ser definido de acordo com a necessidade e a capacidade de armazenamento, não podendo ser inferior a 90 (noventa) dias.

Art. 70. Os softwares de gerenciamento, sistemas operacionais, serviços de infraestrutura de rede e camada de middleware deverão ser regidos pela política de controle de acesso vigente no PJERJ.

SEÇÃO X
DA GESTÃO DE ACESSO AOS BANCOS DE DADOS

Art. 71. O acesso aos dados de sistemas corporativos do PJERJ armazenados em Sistema de Gerenciamento de Banco de Dados (SGBD) deverá ser realizado através de sistema corporativo informatizado, cujas regras são definidas pelo negócio e de acordo com os perfis e papéis de seus usuários.

§ 1º. Nas hipóteses em que o acesso referido nesse artigo requeira ser realizado diretamente em interface do SGBD, exceto para realização de apurações especiais e manutenção de sistemas executados pelo corpo técnico da DGTEC, os seguintes requisitos deverão ser atendidos:

I. ser realizado através de credenciais individualizadas, pessoais e intransferíveis;

II. ser previamente apreciado pelo CGSI e autorizado pelo Presidente do PJERJ, cuja autorização deve conter a justificativa, a finalidade e se a permissão é de leitura e/ou edição de dados;

III. ser realizado através de software licenciado e homologado pela DGTEC;

IV. ser a solicitação registrada em sistema de gestão de requisições de serviços em que conste o nome, matrícula, lotação do solicitante, cópia da autorização de acesso emitida pelo Presidente do PJERJ e especificação da(s) tabela(s), programa(s) e o(s) privilégio(s) necessário(s) (leitura e/ou edição);

V. tal acesso deverá ser concedido com prazo máximo de 30 (trinta) dias, renováveis por igual período e cumprindo o mesmo processo exigido para a concessão.

§ 2º. Os acessos externos as bases de dados realizado através de ferramentas automatizadas deverá seguir os padrões adotados pelo PJERJ e serão monitorados pela DGTEC.

§ 3º. O PJERJ poderá controlar e bloquear acesso externos realizados através de ferramentas automatizadas, para preservar o ambiente computacional e garantir um serviço igualitário a todos os usuários.

Art. 72. Todo acesso a SGBD de sistemas corporativos do PJERJ não realizado através de sistema corporativo informatizado e com fins a alteração de dados armazenados deve ser devidamente registrado em ferramenta de requisições de mudanças oficial da DGTEC (atualmente, o HPSM), incluindo autorização pelo magistrado ou diretor/chefia o qual seja responsável pelo respectivo sistema.

Art. 73. O acesso aos dados armazenados em SGBD do PJERJ através de sistemas corporativos deverá primar pelo controle de acesso individualizado e pessoal, quando a regra de negócio assim exigir, incluindo o devido registro de acesso realizado a dado sigiloso ou em segredo de justiça, assim como deverá incluir proteção de "ataques" de "força bruta" ou de "negação de serviço" que possam sobrecarregar recursos do respectivo SGBD e indisponibilizar outros sistemas corporativos.

Art. 74. Toda senha de acesso a SGBD do PJERJ ou a sistema corporativo informatizado do PJERJ deverá possuir proteção contra leitura em texto aberto, seja ela armazenada em arquivo executável, servidor de aplicação ou no próprio SGBD, seja no seu tráfego pela rede de dados.

Parágrafo único. A atribuição da responsabilidade por preservação e proteção da respectiva senha deverá ser individualizada e documentada, para fins de eventual auditoria.

Art. 75. Toda senha de acesso a SGBD de sistemas corporativos do PJERJ deverá ser alterada trimestralmente. A alteração deverá ser executada durante mudança realizada para manutenção do(s) respectivo(s) sistema(s) corporativo(s) que utilizam aquela senha.

CAPÍTULO IV
DA GESTÃO DE SEGURANÇA DE ACESSO A RECURSOS DE TIC

Art. 76. A DGTEC, após deliberação pelo CGSI e autorização do Presidente do PJERJ, poderá realizar acessos a computadores, servidores, arquivos e registros (logs) para diagnóstico de problemas ou em casos de suspeita de violação de regras, ainda que não autorizados pelo usuário ou chefe do órgão.

Art. 77. As solicitações para auditoria de segurança, análise ou informação quanto ao uso indevido dos recursos de TIC, deverão ser solicitados formalmente à DGTEC, sendo submetidos à deliberação do CGSI e, autorizados pelo Presidente do PJERJ.

Art. 78. Os usuários deverão notificar à DGTEC quaisquer fragilidades ou ameaças, ocorridas ou suspeitas, na segurança dos sistemas, serviços ou informações, mesmo que estas não estejam diretamente sob sua responsabilidade.

§1º. Em nenhuma hipótese o usuário deve realizar uma averiguação de fragilidade de forma autônoma.

§2º. a realização de investigação poderá ser interpretada como potencial uso impróprio do sistema.

Art. 79. A DGTEC deverá dispor de recursos que permitam monitorar, detectar, e identificar atividades indevidas nos recursos de TIC, inclusive as praticadas por usuários internos do PJERJ.

Art. 80. É vedado o compartilhamento de diretórios, arquivos e demais Ativos de TIC, sem prévia autorização da DGTEC.

Parágrafo único. É vedado o acesso por terceiros a qualquer ativo de TIC que possa pôr em risco a integridade, confidencialidade e segurança das atividades do PJERJ, ressalvas exceções legais.

Art. 81. A detecção de compartilhamentos e diretórios que ponham em risco a segurança, implicará a desconexão imediata da estação até o saneamento dos riscos, a apuração de responsabilidade e adoção de providências cabíveis.

Art. 82. O acesso remoto às estações de trabalho, com o objetivo de suporte e manutenção dos recursos de TIC, só poderá ser realizado por equipe autorizada da DGTEC e sempre de forma transparente ao usuário, mediante prévia permissão deste, do chefe do órgão, do CGSI ou do Presidente do PJERJ.

§ 1º. Na hipótese de o usuário estar utilizando a estação de trabalho durante o acesso remoto, este só pode ocorrer com a ciência prévia do usuário.

§ 2º. Não se aplica a regra estabelecida neste artigo as atualizações e correções de sistemas comerciais e corporativos comuns, distribuídos remotamente para todo o parque de equipamentos do PJERJ.

Parágrafo único. A DGTEC deverá autorizar e ter meios para controlar todos os acessos remotos, inclusive os externos, de forma a garantir a segurança do ambiente corporativo.

Art. 83. É vedado dificultar ou impedir a atuação de pessoal autorizado pela DGTEC na execução de procedimentos técnicos nos recursos de TIC.

Art. 84. Cabe à DGTEC, propor ao CGSI as políticas, procedimentos e normas para controlar o trabalho remoto, o acesso e o uso de dispositivos móveis, visando reduzir os riscos de subtração de informações e o acesso não autorizado aos sistemas internos do PJERJ.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 85. Os casos omissos na aplicação dos dispositivos deste Ato Normativo serão objeto de deliberação pelo CGSI e encaminhados ao Presidente do PJERJ para decisão.

Art. 86. O presente Ato Normativo entrará em vigor na data de sua publicação, revogando as disposições em contrário.

Rio de Janeiro, 29 de setembro de 2020.

Desembargador CLAUDIO DE MELLO TAVARES
Presidente

ANEXO
GLOSSÁRIO

AC JUS: é a primeira Autoridade Certificadora no mundo criada e mantida pelo poder judiciário. Foi criada após a edição da MP 2200/2001, que dá validade legal aos documentos assinados com certificados digitais emitidos dentro da hierarquia da ICP-Brasil. O Conselho da Justiça Federal decidiu pela criação de uma Autoridade Certificadora para possibilitar a definição de regras e perfis de certificados, específicos para aplicações do Judiciário. A AC-JUS alavancou definitivamente a implantação da Certificação Digital no Judiciário, com o desenvolvimento de aplicações para comunicação e troca de documentos, agora com validade legal, viabilizando dessa forma o advento do Processo Judicial Eletrônico.

Adware: é um software indesejado projetado para jogar anúncios em sua tela, na maioria das vezes dentro de um navegador da Web.

Blogs: Um blogue (em inglês: blog) (contração de weblog, que era a combinação dos termos em inglês web e log, "diário da rede") é um sítio eletrônico cuja estrutura permite a atualização rápida a partir de acréscimos dos chamados artigos, ou postagens ou publicações.

Chats: Um chat, que em português significa conversação ou mais informalmente bate papo (termo apenas utilizado no Brasil), é um estrangeirismo que designa aplicações de conversação em tempo real.

Data Center: é um ambiente projetado para abrigar servidores e outros componentes como sistemas de armazenamento de dados e equipamentos de rede.

Desktop: Computador de mesa.

Download: Download significa descarregamento, transferência. O uso mais comum do termo download está relacionado com a obtenção de conteúdo da Internet, onde um servidor remoto hospeda dados que são acessados pelos clientes através de aplicativos específicos que se comunicam com o servidor de arquivos através de protocolos preestabelecidos.

Exploits: são um subconjunto de malware. Normalmente, são programas maliciosos com dados ou códigos executáveis capazes de aproveitar as vulnerabilidades de sistemas em um computador local ou remoto

Hacker: Em informática, hacker é um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores. Graças a esses conhecimentos, um hacker frequentemente consegue extrapolar os limites do funcionamento "normal" dos sistemas como previstos pelos seus criadores; incluindo, por exemplo, contornar as barreiras que supostamente deveriam impedir o controle de certos sistemas e acesso a certos dados.

Hoax: Um embuste (Hoax, em inglês) é uma tentativa de enganar um grupo de pessoas, fazendo as acreditar que algo falso é real. Há frequentemente algum objeto material envolvido com aquilo que é realmente uma falsificação; todavia, é possível perpetrar um embuste fazendo somente declarações verdadeiras usando palavreado ou contexto pouco usual. Diferentemente da fraude ou do "conto do vigário" (os quais geralmente têm uma audiência de uma ou de poucas pessoas), e que são perpetrados com o fito de obter ganhos materiais e financeiros ilícitos, um embuste é frequentemente perpetrado como um trote, para causar constrangimento ou para provocar uma mudança social tornando as pessoas cônscias de algo.

Keyloggers: são aplicativos ou dispositivos que ficam em execução em um determinado computador para monitorar todas as entradas do teclado. Assim, aquele que deixou o programa em execução pode, em outro momento, conferir tudo o que foi digitado durante um determinado período.

Log: Em computação, log de dados é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.

Login: Login também é o nome escolhido pelo usuário quando tem que fazer a autenticação para usar um determinado sistema ou serviço. Também pode significar a ação de ter acesso a determinado recurso computacional.

Phishing: é uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e mails falsos ou direcionando você a websites falsos.

Secure Sockets Layer (SSL): É um protocolo de criptografia projetado para internet, que objetiva a transferência de dados de forma segura.

Servidor de Arquivos: Em computação, um servidor de arquivos é um computador conectado a uma rede que tem o objetivo principal de proporcionar um local para o armazenamento compartilhado de arquivos de computadores (como documentos, arquivos de som, fotografias, filmes, imagens, bases de dados, etc.).

Servidor Relay: é um servidor SMTP (Protocolo de Transferência de Correio Simples) configurado de tal forma que permite que qualquer pessoa na internet envie e-mail através dele, não apenas mensagens destinadas a ou provenientes de usuários conhecidos.

Smart card: Cartão inteligente, também conhecido como smart card é um cartão que geralmente assemelha se em forma e tamanho a um cartão de crédito convencional de plástico com tarja magnética. Além de ser usado em cartões bancários e de identificação pessoal, é encontrado também nos celulares (o chip da companhia telefônica).

Smartphones: é um telefone celular, e significa telefone inteligente, em português, e é um termo de origem inglesa. O smartphone é um celular com tecnologias avançadas, o que inclui programas executados um sistema operacional, equivalente aos computadores.

Software: é uma sequência de instruções a serem seguidas e/ou executadas, na manipulação, redirecionamento ou modificação de um dado (informação) ou acontecimento. Normalmente se refere a programas de computador.

Spam: spam é sinónimo de lixo de correio eletrônico e designa mensagens de correio eletrônico com fins publicitários.

Spyware: Um spyware, em português código espião ou programa espião, consiste em um programa automático de computador encontrado também em smartphones, que recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o conhecimento e consentimento do usuário.

Streaming media: A tecnologia streaming é uma forma de transmissão instantânea de dados de áudio e vídeo através de redes. Por meio do serviço, é possível assistir a filmes ou escutar música sem a necessidade de fazer download, o que torna mais rápido o acesso ao conteúdo online.

Tokens: é um dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador, podendo também, em algumas versões, ser conectado a uma porta USB. Existe também a variante para smart cards e smartphones, que é capaz de realizar as mesmas tarefas do token.

URL: Forma padronizada de representação de diferentes documentos, mídia e serviços de rede na internet, capaz de fornecer a cada documento um endereço único.

VOIP: Voice Over Internet Protocol, voz sobre IP é a conversação humana usando a Internet ou qualquer outra rede de computadores baseada em protocolo IP.

Protocolo IP: O IP (Internet Protocol) é o principal protocolo de comunicação da Internet.

Webmail: é uma interface da Internet que permite ao utilizador ler e escrever e mail usando um navegador.

Wiki: é um conceito que se utiliza no âmbito da Internet para fazer referência às páginas web cujos conteúdos podem ser editados por múltiplos utilizadores através de qualquer navegador. Essas páginas, por conseguinte, são desenvolvidas a partir da colaboração das pessoas, as quais podem adicionar, modificar ou eliminar informação. O termo wiki deriva do havaiano wiki wiki, que significa "rápido", e foi proposto por Ward Cunningham. A noção tornou se popular com o auge do Wikipedia, uma enciclopédia livre e aberta que se constituiu com um dos sítios mais visitados da Web.