



**MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL**

INSTRUÇÃO NORMATIVA/INPI/PR Nº 02, DE 24 DE ABRIL DE 2023

Institui a Política de Controle de Acessos aos ativos de informação e à rede de dados corporativos no âmbito do Instituto Nacional da Propriedade Industrial – INPI, em complemento à Política de Segurança da Informação, regulamentada pela Portaria INPI/PR nº 65, de 1º de setembro de 2022.

O PRESIDENTE SUBSTITUTO DO INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL - INPI, no uso das atribuições que lhe conferem o Regimento Interno, aprovado por meio da Portaria do Ministério da Indústria, Comércio Exterior e Serviços (MDIC) nº 11, de 27 de janeiro de 2017, e tendo em vista o previsto na Lei Nº 13.709, de 14 de agosto de 2018; no Decreto nº 9.637, de 26 de dezembro de 2018; no Decreto nº 10.332, de 29 de abril de 2020 e na PORTARIA/INPI/PR nº 65, de 1º de setembro de 2022, assim como o constante nos autos do processo INPI nº 52402.012072/2022-94,

RESOLVE:

Art. 1º Fica aprovada, no âmbito do INPI, a Norma para Criação e Administração de contas de acesso, em complemento às diretrizes estabelecidas pelo Capítulo I, Seção IX, da Política de Segurança da Informação do INPI, PORTARIA/INPI/PR nº 65, de 1º de setembro de 2022.

**CAPÍTULO I
DO ACESSO LÓGICO**

Art. 2º O acesso lógico aos recursos da Rede corporativa do INPI deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela CGTI, baseado nas responsabilidades e tarefas de cada usuário.

§ 1º Terão direito a acesso lógico aos recursos da Rede corporativa do INPI os usuários de recursos de tecnologia da informação.

§ 2º Para fins desta Resolução, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade no INPI.

§ 3º O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações.

**CAPÍTULO II
DA CONTA DE ACESSO LÓGICO E SENHA**

Art. 3º Para utilização das estações de trabalho do INPI, será obrigatório o uso de uma única identificação (login) e de senha de acesso, fornecidos pela CGTI, mediante solicitação formal pelo titular da unidade do requisitante.

§ 1º O formulário de solicitação de acesso se encontra disponível na Intranet do INPI.

§ 2º Os privilégios de acesso dos usuários à Rede corporativa do INPI devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

§ 3º Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para o Serviço de Atendimento ao Usuário e Administração de Rede (SERED) que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 4º O login e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pelo SERED quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 5º O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, carlos.silva.

Parágrafo único. Nos casos de prévia existência de conta de acesso para outro usuário, a CGTI realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 6º O padrão adotado para o formato da senha é o definido pelo CGTI, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

§ 1º A formação da senha da identificação (login) de acesso à Rede corporativa do INPI deve seguir as regras estabelecidas na CGTI e publicadas na intranet.

§ 2º A CGTI fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede corporativa do INPI.

Art. 7º As senhas de acesso serão renovadas a cada 90 (noventa) dias, devendo o usuário ser informado antecipadamente, a fim de que ele próprio efetue a mudança.

Parágrafo único. Caso o usuário não efetue a troca no prazo estabelecido, seu acesso à Rede corporativa do INPI será bloqueado até que nova senha seja configurada.

CAPÍTULO III DO BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 8º A conta de acesso será bloqueada nos seguintes casos:

I - Após 5 (cinco) tentativas consecutivas de acesso errado;

II - Solicitação do superior imediato do usuário com a devida justificativa;

III - Quando da suspeita de mau uso dos serviços disponibilizados pelo INPI ou descumprimento da Política de Segurança da Informação – POSIN e normas correlatas em vigência; e

IV - Após 45 (quarenta e cinco) dias consecutivos sem movimentação pelo usuário.

Art. 9º O desbloqueio da conta de acesso à Rede corporativa do INPI será realizado apenas após solicitação formal do superior imediato do usuário à CGTI.

Art. 10. Quando do afastamento temporário do usuário, a conta de acesso deverá ser bloqueada a pedido do superior imediato ou do CGRH.

Art. 11. A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

CAPÍTULO IV DA MOVIMENTAÇÃO INTERNA

Art. 12. Em caso de mudança do usuário para outro setor, os direitos de acesso à Rede corporativa do INPI a serem cancelados e/ou habilitados para o servidor devem ser devidamente informados no processo de remoção no SEI (Sistema Eletrônico de Informações).

§ 1º A Coordenação-Geral de Recursos Humanos (CGRH) do INPI deverá enviar os processos de remoção à CGTI para informar sobre a atualização dos acessos (cancelamento e/ou habilitação) à Rede corporativa do INPI a ser efetuada, mediante formulário específico.

§ 2º Os cancelamentos e habilitações de acesso do usuário de que trata o caput serão informados, respectivamente, pela atual chefia imediata e pela futura chefia imediata no formulário de remoção específico.

CAPÍTULO V DA CONTA DE ACESSO BIOMÉTRICO

Art. 13. A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

Parágrafo único. O INPI deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VI DOS ADMINISTRADORES

Art. 14. A utilização de identificação (login) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

§ 1º Somente os técnicos da CGTI, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

§ 2º Na necessidade de utilização de login com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para o CGTI, que poderá negar os casos em que entender desnecessária a utilização.

§ 3º Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, sendo vedado instalar, desinstalar ou remover qualquer programa sem autorização formal da CGTI.

§ 4º Caso constatada alguma irregularidade, o usuário perderá o acesso como administrador, salvo casos avaliados pela CGTI.

§ 5º A identificação (login) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

§ 6º Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

§ 7º Excepcionalmente, poderão ser concedidas identificações (login) de acesso com privilégio de administrador à rede de comunicação de dados a visitante, em caráter temporário, após autorização da CGTI.

§ 8º O padrão adotado para o formato da conta de acesso administrador é adm_login.

CAPÍTULO VII DAS RESPONSABILIDADES

Art. 15. É de responsabilidade do superior imediato do usuário comunicar formalmente à CGTI o desligamento ou saída do usuário do INPI para que as permissões de acesso à Rede corporativa do INPI sejam canceladas.

Art. 16. Caberá à CGRH do INPI a comunicação imediata à CGTI sobre desligamentos e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

Art. 17. É responsabilidade do Serviço de Administração Predial e Atividades Auxiliares (SAPRA) do INPI a comunicação imediata à CGTI da Informação sobre desligamentos e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

Parágrafo único. Em havendo contrato de empresas prestadoras de serviços cuja gestão não seja feita pelo SAPRA a responsabilidade mencionada no caput caberá ao Gestor do respectivo contrato.

Art. 18. É de responsabilidade da Divisão de Segurança da Informação do INPI o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do INPI.

Parágrafo único. Os serviços de que trata o caput serão filtrados por programas de antivírus, anti-phishing e anti-spam e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.

Art. 19. O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede corporativa do INPI e a recursos de tecnologia custodiados ou de propriedade do INPI.

Art. 20. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

Art. 21. A utilização simultânea da conta de acesso à Rede corporativa do INPI em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

Art. 22. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem suas credenciais de acesso.

Art. 23. O usuário deve informar à CGTI qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 24. É dever do usuário zelar pelo bom uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I - Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II - Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III - Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV - Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V - Não divulgar a terceiros ou a outros usuários os dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI - Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII - Não instalar aplicativo ou programa em computadores do INPI sem prévia autorização da CGTI.

VIII - Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

IX - Assinar o Termo de Responsabilidade (Modelo - Anexo A) quanto à utilização da respectiva conta de acesso.

CAPÍTULO VIII **DISPOSIÇÕES FINAIS**

Art. 25. Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários à CGTI e/ou chefe imediato.

Art. 26. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Divisão de Segurança da Informação – DISEG fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

Parágrafo único. Nos casos em que o ator da quebra de segurança for um usuário, a DISEG comunicará os resultados ao superior imediato do mesmo para adoção de medidas administrativas cabíveis.

Art. 27. Ações que violem a POSIN ou que quebrem os controles de Segurança da Informação serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

Art. 28. Processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela POSIN.

Art. 29. Os casos de violação/transgressão omissos nas legislações correlatas serão resolvidos pelo Comitê de Segurança da Informação - CSI do INPI.

Art. 30. Fica revogada a Resolução INPI/PR nº 07, de 15 de março de 2013.

Art. 31. Esta Instrução Normativa entra em vigor no dia 15 de maio de 2023.



Documento assinado eletronicamente por **JULIO CESAR CASTELO BRANCO REIS MOREIRA, Presidente**, em 08/05/2023, às 15:32, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.inpi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0808051** e o código CRC **99529303**.

ANEXO A

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ deste Instituto, 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 INPI;
- II. Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INPI.;
- 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 27 de maio de 2020, que Dispõe sobre Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- IV. Utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INPI.;
- V. Responder, perante o INPI., pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;
- VI. Acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;
- VII. Utilizar o correio eletrônico (e-mail) colocado a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;
- VIII. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;
- IX. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

X. Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (browser), bloquear estação de trabalho, bem como encerrar a seção do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

XI. Não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou do correio eletrônico (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

XII. Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

, ____ DE _____ DE _____.

ASSINATURA
NOME DO USUÁRIO E SEU SETOR ORGANIZACIONAL

NOME DA AUTORIDADE RESPONSÁVEL PELA AUTORIZAÇÃO DO ACESSO