CÓDIGO de CONDUTA e SEGURANÇA

versão 02.2024 – 01/agosto/2024.

GESTÃO PARA RESULTADOS

Responsabilidade jurídica e LGPD:
Ana Cláudia Ferigato
Advogada e Consultora

Rua irmã Gabriela, 51, Cidade Monções
CEP: 04571-130 • São Paulo/SP
Telefone: +55 (11) 5509-7700

www.fnq.org.br

SUMÁRIO

Versão 01/2024 – agosto 2024.

Prefácio do Código de Conduta da FNQ 01

Carta Aberta aos Colaboradores e Prestadores de Serviço 01

Compromisso com a Ética e a Transparência 01

Conformidade com a LGPD e Segurança de Dados 02

Políticas de Compliance e Prevenção à Corrupção 02

Aplicabilidade e Cumprimento 02

Compromisso com a Excelência 03

CÓDIGO DE CONDUTA FNQ 04

1. A QUEM SE DESTINA 04

a. Colaboradores 04

b. Prestadores de Serviço 04

c. Fornecedores e Parceiros 04

d. Clientes e Consumidores 04

e. Outras Partes Interessadas 04

1.1. OBJETIVOS DO CÓDIGO DE CONDUTA 05

2. SEGURANÇA DA INFORMAÇÂO 05

2.1. PRINCÍPIOS E REGRAS DE SEGURANÇA DA INFORMAÇÃO 05

2.2. CONCESSÃO, REVOGAÇÃO E REVISÃO ,,,, ... 06

2.3. USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO 06

2.4. PERMISSÕES DIFERENCIADAS e IDENTIDADES DE ACESSO 07

2.5. VEDAÇÕES 07

2.6. GESTÃO DE INFORMAÇÕES 09

2.7. GESTÃO DE IDENTIDADE 11

2.8. ACESSO À INTERNET 12

2.9. CORREIO ELETRÔNICO 13

2.10. DISPOSITIVOS MÓVEIS E ACESSO REMOTO 15

2.11. HOME OFFICE 15

2.12. *BACKUPS* *16*

3. PROTEÇÃO DE DADOS PESSOAIS *16*

3.1. TRATAMENTO DE DADOS E BASES LEGAIS 16

3.2. DIREITOS DO TITULAR 18

3.3. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 18

3.4. ARMAZENAMENTO E DESCARTE DE INFORMAÇÕES FÍSICAS 19

3.5. TREINAMENTO 19

4. OUTRAS DISPOSIÇÕES 20

4.1. IDENTIFICAÇÃO VISUAL 20

4.2. CARTÃO DE ACESSO 20

4.3. CERTIFICADO DIGITAL 20

4.4. MONITORAÇÃO E INSPEÇÃO 21

4.5. IMPRESSÃO 21

4.6. MESA LIMPA e TELA LIMPA 22

5. PAPÉIS E RESPONSABILIDADES 23

a. Diretores e gestores: 23

b. Responsável de TI: 23

c. Responsável do RH: 24

d. Responsável pelas questões jurídicas: 24

e. Gestor responsável pelo *Colaboradores* e *Prestadores de Serviço*: 24

f. *Colaboradores* e *Prestadores de Serviço* 25

g. Encarregado de dados: 25

h. Comitê de Segurança e Privacidade de Dados: 26

6. PROCESSO DISCIPLINAR 27

a. Recebimento da Denúncia ou Identificação da conduta 27

b. Análise Preliminar 27

c. Instauração do Processo Disciplinar 27

d. Investigação Formal 28

e. Conclusão da Investigação 28

f. Decisão e aplicação de medidas Disciplinares. 28

g. Encerramento do Processo 28

7. DISPOSIÇÕES FINAIS 28

8. DA APROVAÇÃO 29

APÊNDICE 30

A. Glossário de termos. 30

Rua irmã Gabriela, 51, Cidade Monções
CEP: 04571-130 • São Paulo/SP
Telefone: +55 (11) 5509-7700

www.fnq.org.br

Carta Aberta aos Colaboradores e Prestadores de Serviço.

Versão 01/2024 – agosto 2024.

Prezados *Colaboradores* e *Prestadores de Serviço*,

A Fundação Nacional da Qualidade - FNQ como entidade privada, qualificada como organização de utilizade pública, sem fins lucrativos e em atuação desde 1991, conta com uma equipe própria, rede de clientes, parceiros, apoiadores e voluntários em torno de sua causa: *a busca contínua da excelência por meio da Gestão, Inovação e Ciência, e a consequente contribuição para o aumento da produtividade das organizações e da competitividade do País, com ética e sustentabilidade*.

Temos como pilares fundamentais a transparência, a ética e a excelência em todas as suas relações e operações. Nosso compromisso é com a integridade e a conformidade em todos os processos e áreas de atuação da FNQ, como também, no que tange à proteção de dados pessoais de todos os envolvidos.

Vocês, nossos *colaboradores* e *prestadores de serviço*, são a linha direta de atuação da FNQ e, portanto, desempenham um papel crucial na manutenção e promoção desses valores. É através de suas ações diárias que nossos princípios se materializam e ganham vida.

Cada um de vocês é responsável por assegurar que nossas práticas sejam conduzidas de maneira íntegra e transparente, refletindo o compromisso da FNQ com a ética e a qualidade. A responsabilidade que vocês, como *Colaboradores* e *Prestadores de Serviço*, carregam não é apenas uma expectativa, mas uma obrigação fundamental para o sucesso e a reputação da nossa organização.

Desta forma, são todos *Colaboradores* e *Prestadores de Serviços* os guardiões dos valores da FNQ, e é essencial que cada decisão, cada interação e cada processo sejam conduzidos com a máxima integridade e respeito às normas estabelecidas, como pontualmente apresentamos a seguir.

Compromisso com a Ética e a Transparência

A FNQ proíbe rigorosamente qualquer forma de corrupção, fraude, suborno, favorecimento e extorsão, seja por parte de seus colaboradores, clientes, fornecedores ou parceiros. Nossa missão inclui a obrigação de restringir o acesso a dados confidenciais e sensíveis, protegendo-os contra perdas ou comprometimentos que possam causar impactos adversos aos nossos clientes, colaboradores, fornecedores, parceiros e à própria FNQ.

Responsável pela Política em adequação à LGPD.
Ana Cláudia Ferigato
Advogada e Consultora LGPD.

Além disso, estamos comprometidos em garantir a transparência em todas as nossas ações e decisões, promovendo um ambiente de trabalho ético e justo.

Conformidade com a LGPD e Segurança de Dados

Temos um compromisso assumido para que os titulares de dados tenham acesso adequado às suas informações, conforme necessário para o funcionamento eficaz de nossas operações. Com isso, estabelecemos nesta política as regras e orientações para a utilização segura e ética dos dados, em conformidade com a Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018.

Nosso objetivo é minimizar incidentes e ações danosas aos dados pessoais, aumentar a conscientização dos usuários e evitar cenários de perda acidental, embora reconheçamos que a eliminação de todos os riscos não é possível.

Políticas de Compliance e Prevenção à Corrupção

Além da proteção aos Dados Pessoais, a FNQ adota políticas rigorosas de compliance para assegurar que todos os processos internos estejam em conformidade com as normas legais e regulamentares aplicáveis.

Implementamos políticas antissuborno e anticorrupção que visam prevenir, detectar e responder a quaisquer atos ilícitos ou antiéticos.

Todos vocês, *Colaboradores* e *Prestadores de Serviço*, além também de nossos parceiros, são orientados e treinados para seguir essas diretrizes, garantindo que nossas operações sejam conduzidas de maneira íntegra e responsável.

Aplicabilidade e Cumprimento

Esta política detalha os requisitos para a prevenção de *violações de dados* e *práticas antiéticas* que facilitem a *corrupção*, *fraudes, subornos* ou qualquer tipo de *vantagem indevida* que cause ou possa causar a *invalidação* ou *anulação* de qualquer processo interno ou externo da FNQ, visando à proteção dos dados pessoais de nossa base de clientes, colaboradores e demais envolvidos, além de boas práticas e regras de *Compliance* nacional ou internacional.

Para isso, a política aqui estabelecida deve ser rigorosamente cumprida por todas as partes envolvidas nas atividades vinculadas à FNQ e é aplicável a todos os processos e dados dos titulares, sejam dados pessoais (gerais ou sensíveis), servidores, bancos de dados e sistemas de TI que lidam com esses dados, incluindo qualquer dispositivo utilizado regularmente.

Outrossim, informações classificadas como *públicas* não estão sujeitas a esta política, e dados correlacionados podem ser excluídos da mesma, com base em necessidades específicas de negócios, visando proteger dados de alto custo ou muito complexos.

Compromisso com a Excelência

Este é um documento com valor jurídico e aplicabilidade imediata e indistinta a todos que venham a ter acesso a dados pessoais e/ou recursos tecnológicos da FNQ.

Reforçamos nosso compromisso com a transparência, ética, conformidade e excelência, e contamos com a colaboração de todos para mantermos nossos princípios e valores sempre presentes em nossas atividades diárias.

Atenciosamente,

Fundação Nacional da Qualidade - FNQ

Para mais informações sobre nossa visão, valores e princípios, visite nosso site.

1. A QUEM SE DESTINA

O Código de Conduta é um documento essencial para a organização e é destinado a todos os indivíduos e entidades que interagem com esta, de maneira direta ou indireta.

Seu objetivo é o de fornecer diretrizes claras sobre comportamentos aceitáveis e inaceitáveis, procedimentos a serem seguidos e as consequências do não cumprimento dessas regras. Além disso, tem como objetivo alinhar as condutas de todos os membros, *Colaboradores* ou *Prestadores de Serviço,* aos padrões de proteção de dados pessoais e ajudar a garantir que todos os membros da organização ajam de acordo com os valores e princípios estabelecidos no Código de Ética.

Seus principais destinatários incluem:

a. Colaboradores

- **Funcionários em Geral:** Todos os empregados, independentemente de sua posição hierárquica ou departamento, devem seguir as diretrizes estabelecidas no Código de Conduta.
- **Gestores e Executivos:** Líderes e gestores têm um papel crucial em exemplificar e reforçar as normas de conduta, além de garantir que suas equipes as sigam.

b. Prestadores de Serviço

- **Consultores e Contratados:** Qualquer pessoa ou empresa que preste serviços à organização deve aderir às normas e práticas descritas no Código de Conduta.
- **Terceirizados:** Empresas e profissionais terceirizados que atuam em nome da organização também devem cumprir as diretrizes estabelecidas.

c. Fornecedores e Parceiros

- **Fornecedores de Produtos e Serviços:** Empresas que fornecem bens ou serviços para a organização devem seguir as normas de conduta, especialmente em aspectos relacionados à ética e à conformidade.
- **Parceiros de Negócios:** Qualquer entidade que colabore ou tenha uma parceria estratégica com a organização deve estar alinhada com as práticas e valores descritos no Código de Conduta.

d. Clientes e Consumidores

- **Clientes:** Embora o foco principal do Código de Conduta seja interno, clientes e consumidores também podem ser impactados, pois o documento assegura que a empresa atua de maneira ética e transparente em suas interações e transações.

e. Outras Partes Interessadas

- **Investidores e Acionistas:** Demonstrar que a empresa possui e segue um Código de Conduta pode aumentar a confiança e a credibilidade junto aos investidores e acionistas.
- **Órgãos Reguladores e Governamentais:** O cumprimento das normas de conduta pode facilitar a conformidade com regulamentos e leis, além de melhorar a relação com órgãos reguladores.

1.1. OBJETIVOS DO CÓDIGO DE CONDUTA

- **Orientar Comportamentos:** Estabelecer expectativas claras sobre comportamentos aceitáveis e inaceitáveis no ambiente de trabalho.
- **Promover a Ética:** Assegurar que todos os membros da organização ajam de maneira ética e responsável.
- **Garantir Conformidade:** Ajudar a organização a cumprir leis e regulamentos aplicáveis.
- **Proteger a Reputação:** Manter e proteger a reputação da organização através de práticas transparentes e éticas.

O Código de Conduta é um instrumento vital para garantir que todos os indivíduos e entidades associadas à organização sigam os mesmos padrões de comportamento ético e profissional. Ele é destinado a uma ampla gama de destinatários, incluindo colaboradores, prestadores de serviço, fornecedores, parceiros, clientes e outras partes interessadas, assegurando que a cultura de integridade e responsabilidade permeie todas as áreas da organização.

2. SEGURANÇA DA INFORMAÇÂO

A segurança da informação é fundamental para proteger os ativos da FNQ e assegurar a continuidade das operações.

Este tópico estabelece os princípios, definições e regras para a segurança da informação, que devem ser seguidos por todos os *Colaboradores* e *Prestadores de Serviço*.

2.1. PRINCÍPIOS E REGRAS DE SEGURANÇA DA INFORMAÇÃO

Todas as informações geradas, acessadas, manuseadas, armazenadas, compartilhadas ou descartadas no exercício das atividades realizadas FNQ são de propriedade e direito de uso exclusivo da FNQ, sendo responsabilidade desta zelar para que informações inseridas nos sistemas, ou quando enviadas a qualquer contato externo, sejam livres de erro, transparentes e sejam verídicas.

No caso do *Colaborador*, o acesso e uso das informações da FNQ, incluindo o e-mail, devem estar limitados à jornada de trabalho ou período contratual deste, exceto quando exercer atividade justificada ou plantões específicos devidamente controlados.

Quando necessária troca de informações com os clientes para cumprimento legal de obrigações, é necessário utilizar os canais oficiais disponibilizados pela FNQ e cliente.

Qualquer canal distinto ao correio eletrônico (e-mail), mensageiro eletrônico e sistema de arquivos oferecidos pela FNQ será considerado como descumprimento das regras de segurança da informação e serão tomadas as medidas cabíveis quanto ao fato.

2.2. CONCESSÃO, REVOGAÇÃO E REVISÃO

- **Concessão de Acessos:** Os acessos a sistemas e informações serão concedidos com base na necessidade de cada função, seguindo o princípio do menor privilégio. A concessão de acesso aos recursos tecnológicos da **FNQ** deve estar atrelada aos perfis de acesso previamente atribuídos ao colaborador em razão da atividade exercida.

A solicitação de acesso deve ser realizada pelo gestor do colaborador ao responsável de TI via sistema de chamados com todas as informações do usuário cadastrado.

- **Revisão de Acessos:** A revisão periódica dos acessos é obrigatória para garantir que apenas as pessoas autorizadas tenham acesso às informações e sistemas. O responsável de TI se reserva o direito de revalidar as permissões, ou não, caso a concessão tenha mais permissões do que o definido em política interna para a efetiva concessão.

Todos os acessos concedidos serão revisados, no mínimo, a cada 6 (seis) meses, a fim de garantir que continuam ativos e atualizados.

- **Revogação de Acessos:** Os acessos devem ser revogados imediatamente quando um colaborador ou prestador de serviço não necessitar mais deles, seja por mudança de função ou desligamento.

A revogação de acesso deve ocorrer mediante solicitação do gestor responsável pelo colaborador ou parceiro ao responsável de TI. No entanto, os direitos de acesso podem ser alterados e/ou revogados a qualquer tempo sem a necessidade de aviso prévio, desde que fundamentados, além de encerramento das atividades entre a **FNQ** e as partes envolvidas.

2.3. USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

O *Colaborador* ou *Prestador de Serviço* deve utilizar apenas *softwares* e *hardwares* previamente homologados ou autorizados pela **FNQ**.

A gestão (instalação, manutenção e configuração) de todos os recursos tecnológicos é de responsabilidade exclusiva da **FNQ**, através de seu setor de Tecnologia.

- **Tela Limpa:** Todo *Colaborador* ou *Prestador de Serviço* que se distanciar de sua estação de trabalho ou do dispositivo móvel, deve imediatamente realizar o processo de **bloqueio do equipamento** garantindo que informações pessoais, sensíveis ou não, além de informações privilegiadas, confidenciais e reservadas, não sejam expostas ou deixadas visíveis em suas telas quando não estiverem em uso ou quando pessoas não autorizadas estiverem por perto.

Os equipamentos disponibilizados aos *Colaboradores* ou *Prestadores de Serviço* são de propriedade da **FNQ**, cabendo a cada um utilizá-los e manuseá-los corretamente, bem como cumprir as recomendações e normas.

As estações de trabalho e servidores contêm softwares de antivírus instalados, ativados e atualizados permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar imediatamente o responsável do setor de TI.

Documentos imprescindíveis para as atividades dos colaboradores deverão ser salvos em drives de rede autorizados previamente, sendo vedado que arquivos relacionados à FNQ e sua atividade sejam apenas gravados localmente em qualquer equipamento, pois não terão garantia de backup (recuperação), podendo estar aberto a qualquer tipo de incidente de segurança.

Caso ocorra qualquer tipo de *incidente de segurança* com arquivos disponibilizados pela FNQ para o exercício profissional de *Colaboradores e Prestadores de Serviço*, será aberta auditoria para apuração da responsabilidade pessoal do usuário sobre o ocorrido.

Em caso de incidente de segurança, os *Colaboradores e Prestadores de Serviço* deverão informar o ocorrido imediatamente ao responsável do setor de TI, indicando dispositivo ou movimentação estranha conectada ou relacionada ao seu equipamento.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução ou auxílio do responsável de TI.

2.4. PERMISSÕES DIFERENCIADAS e IDENTIDADES DE ACESSO

As permissões de acesso serão diferenciadas de acordo com as responsabilidades e necessidades específicas de cada função cargo, conforme interesse da FNQ.

Excepcionalmente, podem ser concedidas autorizações adicionais, temporárias ou não, aos demais colaboradores e parceiros, desde que tal solicitação seja aprovada, justificada e necessária para a execução de determinadas tarefas ou projetos.

2.5. VEDAÇÕES

Quaisquer dos atos ou práticas relacionados a seguir, constitui e são considerados como violação grave do Código de Conduta e resultará em medidas disciplinares severas, que podem incluir o desligamento da organização, inclusive por justa causa, e possíveis ações legais. Desta forma, *Colaboradores* e *Prestadores de Serviço* da FNQ não devem:

a. Se não for atividade relacionada à sua função, realizar qualquer tipo de manutenção ou reparo nos recursos tecnológicos corporativos, sendo estas afetas, exclusivamente ao responsável de TI;

b. Utilizar programas não autorizados ou que deem causa à Evasão de Segurança, ou seja, software, ferramenta ou técnica que tenha como objetivo burlar ou contornar os

controles de segurança implementados pela FNQ. Isso inclui, mas não se limita a, programas que tentem desativar ou evitar sistemas de autenticação, firewalls, monitoramento de rede, ou qualquer outro mecanismo de segurança.

c. Executar programas de compartilhamento de arquivos ou estrutura diversa que permita a interconexão entre usuários de diversas localidades por meio de redes públicas, exceto quando prévia e expressamente autorizado;

d. Acessos de *site* que realizem o redirecionamento de tráfego (proxy) e burlem as políticas digitais;

e. Desinstalar ou desabilitar softwares instalados nos recursos tecnológicos pela FNQ, independentemente do motivo;

f. Acessar informações confidenciais sem explícita e expessa autorização do responsável;

g. Vigiar secretamente outrem por dispositivos eletrônicos ou *softwares,* autorizados ou não;

h. Interromper servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

i. Usar qualquer tipo de recurso tecnológico para facilitar, cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

j. Hospedar, acessar e compartilhar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país.

k. Utilizar *software* não registrado ou sem licença de origem, dito “pirata”, atividade considerada delituosa de acordo com a legislação nacional.

l. Realizar a transferência e/ou a divulgação de qualquer software, programa ou dados para terceiros, por qualquer meio de comunicação (físico ou digital), sem a devida identificação do solicitante, e, verificada esta positivamente, estiver de desacordo com a classificação de tal informação e com a real necessidade do destinatário.

m. Armazenar arquivos pessoais e/ou não pertinentes ao negócio (fotos, músicas, vídeos etc.) para os drives de rede, de forma a poder sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, facultando a organização a prévia comunicação ao usuário e medidas de salvaguarda ou ressarcimento eventualmente aplicáveis.

n. Utilizar dispositivos removíveis de armazenamento de informações (*pen drives*, CDs, DVDs, HD externo) para o transporte de informações. Em caso de extrema necessidade ou exceções, deverá acionar o responsável de TI para validação junto ao gestor responsável e, se autorizado, o dispositivo a ser utilizado deverá conter

tecnologia de criptografia. Por fim, todo o conteúdo transportado deve ser armazenado na rede corporativa e apagado do dispositivo imediatamente após a utilização deste.

o. Consumir alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos eletrônicos.

p. Fazer *download* e utilizar programas de entretenimento, como jogos ou músicas, em equipamentos de propriedade e uso da FNQ.

q. Acessar, armazenar, utilizar ou compartilhar conteúdo agressivo, ofensivo, difamatório, calunioso, constrangedor, violento, abusivo, homofóbico, racista ou político que represente quebra de confidencialidade das informações da FNQ ou de seus clientes; que ainda caracterize assédio moral ou sexual, incite a prática de crimes ou contravenções penais; que constitua violação aos direitos de propriedade intelectual ou industrial da FNQ, bancos de dados, segredos de negócio, dados contábeis ou financeiros, ou de terceiros, incluindo a proteção de suas marcas e patentes, denote ou estimule a perseguição preconceituosa baseada em cor, sexo, raça, incapacidade física ou mental, condição social, origem, religião ou outras situações protegidas pelas leis brasileiras.

2.6. GESTÃO DE INFORMAÇÕES

Todas as informações sigilosas, sejam elas físicas ou digitais, independente do formato ou local de armazenamento, da FNQ ou de seus clientes, devem ser classificadas e rotuladas de forma a permitir fácil identificação e o tratamento adequado, ficando claro quem pode ter acesso a ela e qual o nível de proteção que deve receber.

Informações confidenciais são aquelas que requerem tratamento especial, de conteúdo estratégico, contábil, financeiro, dados pessoais e críticos que, se divulgada, poderá violar a privacidade de indivíduos, revelar segredos de negócio dos nossos clientes, reduzir a vantagem competitiva da FNQ ou causar impactos graves, sob o aspecto financeiro, legal, normativo, de reputação e de imagem aos nossos clientes.

Os *Colaboradores* e *Prestadores de Serviço* devem tratar como CONFIDENCIAL toda a informação que não estiver classificada, e comunicar ao gestor imediato, até que se defina ou se tenha conhecimento da sua classificação adequada.

O tratamento de informação classificada como CONFIDENCIAL deve atender os seguintes requisitos:

a. Estar rotulada como FNQ em todas as páginas, além de identificar *Colaboradores* e *Prestadores de Serviço* e/ou grupos autorizados para o acesso (físico e/ou digital);

b. Autorizar acesso apenas aos *Colaboradores* e *Prestadores de Serviço* previamente identificados;

c. Aplicar medidas de proteção lógica e física que garantam o acesso exclusivo pelos *Colaboradores* e *Prestadores de Serviço* autorizados;

d. Manter sigilo sobre o conteúdo ou informação para demais *Colaboradores* e *Prestadores de Serviço,* além de pessoas não autorizadas;

e. Por meios digitais, o compartilhamento deve ocorrer somente com autorização do gestor imediato e por meio dos recursos tecnológicos da FNQ;

f. Em caso de compartilhamento de documentos por meio de dispositivos de armazenamento móveis (*pen drives*, HDs externo, etc), a mídia deve conter aplicação de criptografia com nível de segurança compatível com o *Advanced Encryption* Standard (AES) ou superior;

g. Possibilitar a eliminação de maneira que impossibilite a posterior recuperação do acesso à informação.

h. Somente é permitida a divulgação de qualquer informação da FNQ ou de seus clientes, quando:

- a divulgação é permitida expressamente por lei e há autorização prévia por escrito;
- a divulgação é exigida por lei, mas desde que seja autorizado previa e formalmente;
- há o dever ou direito profissional de divulgação, mas desde que não proibido por lei e autorizado prévia e formalmente. No entanto, ao se decidir pela divulgação da informação, a FNQ deve considerar se os interesses de terceiros, incluindo partes cujos interesses podem ser afetados, podem ser prejudicados;
- o tipo de comunicação que é esperado, a forma e mídia de divulgação, para quem deve ser dirigida; e
- se as partes para quem a comunicação é dirigida são as pessoas apropriadas para recebê-la.

A necessidade de sigilo profissional permanece mesmo após o término das relações profissionais entre a FNQ e o colaborador ou parceiro.

Assim, é proibido o uso ou compartilhamento de qualquer informação obtida, recebida ou gerada em decorrência do relacionamento profissional. Informação classificada como CONFIDENCIAL não deve ser publicada na internet ou nas mídias sociais.

- Não é permitido realizar o *upload* (transmitir arquivos) ou compartilhamento de informação, pessoais ou confidenciais, da FNQ ou de seus clientes para serviços e aplicativos de comunicação instantânea, de armazenamento na nuvem ou

repositórios digitais, a exemplo, mas não se limitando a *Whatsapp*, *SnapChat*, *Viber*, *Facebook*, *Messenger*, *Telegram, Google Drive*, *OneDrive*, *Dropbox*, *iCloud*, *Box*, *SugarSync*, *Slideshare* e *Scribd*, com exceção dos recursos tecnológicos disponibilizados e homologados pela empresa.

Informações confidenciais não devem ser discutidas, exibidas ou compartilhadas em ambientes públicos ou de livre acesso, onde pessoas alheias à FNQ possam tomar conhecimento. Antes do envio de informações confidenciais, independente se de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou outros meios, o colaborador deve confirmar a identidade e idoneidade do solicitante e a real necessidade do compartilhamento da informação solicitada.

Em caso de dúvida, deve contatar o seu gestor imediato ou responsável de TI.

Informações confidenciais contidas em papéis, recursos tecnológicos e outras formas de suporte de dados não podem ficar expostas em mesas de trabalho, *flipcharts*, impressoras, fax, *scanner*, telas de computadores e nas salas de reunião, principalmente quando não estiverem sendo utilizadas.

A respeito da Confidencialidade obrigatória de informações, cada *Colaborador* e *Prestador de Serviço* deverá assinar um Acordo de Confidencialidade (*Non Disclosure Agreement*) específico para exercício de toda e qualquer função.

2.7. GESTÃO DE IDENTIDADE

A identidade digital concedida ao colaborador ou parceiro é composta por um identificador único (ID ou nome) e por um mecanismo de autenticação sigiloso (senha, biometria, *token*), sendo exclusiva e não pode ser compartilhada com outra pessoa.

O responsável de TI irá configurar o primeiro acesso do colaborador atribuindo uma senha temporária de modo que seja obrigatória sua alteração em seguida da autenticação.

A senha deve ser tratada de forma individual, sigilosa e intransferível, não podendo ser compartilhada ou divulgada a terceiros. A senha não deve ser armazenada nos computadores ou dispositivos móveis, anotadas em papel ou em qualquer outro suporte físico ou eletrônico.

As senhas dos *colaboradores* devem conter, pelo menos, 8 caracteres, dentre letras maiúsculas e minúsculas, números e símbolos;

- não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento;
- não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Já os usuários que possuem *perfil de administrador* ou acesso privilegiado deverão utilizar uma senha de no mínimo 12 caracteres, dentre letras maiúsculas e minúsculas, números e símbolos; sempre que houver suporte à autenticação multifator (MFA) a mesma deve ser habilitada e ser trocada entre 30 e 120 dias, não ser idêntica às últimas 5 utilizadas; ser alterada em qualquer caso de suspeita do comprometimento de seu sigilo ou vazamento.

2.8. ACESSO À INTERNET

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. A FNQ, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os *Colaboradores* e *Prestadores de Serviço* devem estar sempre atentos ao uso da internet e utilizar somente sites confiáveis e com o conteúdo relacionado às atividades da FNQ.

Da mesma forma, todo *Colaboradores* e *Prestadores de Serviço* deve ter extrema atenção quando do recebimento de arquivos executáveis, telas para acesso automático, solicitação de informações cadastrais na Internet, promoções exageradamente vantajosas, e outras atividades suspeitas de *phishing*.

Não é permitido obter e/ou conceder acesso não autorizado, monitorar, interceptar, desativar, sobrecarregar, obstruir ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de examinar ou testar vulnerabilidades em sistemas internos ou externos.

A FNQ autoriza o uso moderado da internet desde que não prejudique a atenção do *Colaboradores* e *Prestadores de Serviço* durante a execução das suas atividades e a qualidade no desempenho de suas funções.

Não é permitida a utilização dos recursos tecnológicos com fins de entretenimento, como por exemplo, acesso a blogs, fotologs, salas de bate-papo, comunicadores instantâneos ou mídias sociais. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da FNQ, que pode analisar e, se necessário, bloquear qualquer arquivo, *site*, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privados da rede, visando assegurar o cumprimento de sua política.

A FNQ, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor.

O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a organização cooperará ativamente com as autoridades competentes.

É proibida a divulgação e/ou o compartilhamento indevido de informações em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os *Colaboradores* e *Prestadores de Serviço* não poderão utilizar os recursos da FNQ para deliberadamente propagar qualquer tipo de vírus, *worm*, cavalo de troia, *spam*, assédio, perturbação ou programas de controle de outros computadores, neste caso, somente o responsável de TI tem permissão para acessar e utilizar programas de acesso remoto a outros computadores.

2.9. CORREIO ELETRÔNICO

O uso do correio eletrônico da FNQ é para fins corporativos e relacionados às atividades do colaborador ou parceiro dentro da organização.

Não é permitido o uso de correio eletrônico particular, a exemplo de Hotmail, Yahoo, Bol, Gmail, outros, para o envio e recebimento de informações da FNQ e seus clientes.

O *Colaboradores* e *Prestadores de Serviço* devem utilizar adequadamente sua caixa postal corporativa, evitando que mensagens deixem de ser lidas ou fiquem sem resposta por mais de 24h em dias úteis.

Os *Colaboradores* e *Prestadores de Serviço* devem organizar e efetuar a limpeza de sua caixa postal corporativa periodicamente, com o fim de evitar problemas de segurança e armazenamento, de modo a eliminar mensagens que, não tenham relação com o trabalho, ou que apresentem conteúdo suspeito que possam levar à eventual infecção da máquina por código malicioso.

Os *Colaboradores* e *Prestadores de Serviço* devem verificar com atenção o endereço de correio eletrônico escolhido como destinatário para evitar o envio de mensagem para pessoa errada e que ocorra vazamento de informações da FNQ, de seus clientes e colaboradores. Contudo, se isso ocorrer, o *Colaboradores* e *Prestadores de Serviço* devem enviar imediatamente outra mensagem solicitando à pessoa que desconsidere a mensagem anterior e a exclua, pois aquele conteúdo não era destinado a ela, e comunicar o responsável de TI sobre o ocorrido.

É vedado aos *Colaboradores* e *Prestadores de Serviço*:

a. Enviar mensagem eletrônica para um número indeterminado ou excessivo de destinatários, exceto quando autorizado e desde que esteja relacionado às atividades contratadas pela FNQ;

b. Divulgar o endereço de e-mail corporativo para fins de recebimento de mensagens pessoais ou de entidades alheias aos interesses ou às atividades prestadas à FNQ;

c. Falsificar informações de endereçamento ou adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

d. Apagar mensagens eletrônicas necessárias à FNQ, sobretudo quando a mesma estiver sujeita a algum tipo de investigação, auditoria ou que possa ser prejudicada em procedimento judicial ou administrativo;

e. Encaminhar ou abrir mensagens consideradas suspeitas ou caracterizadas como corrente, *spam* e *phishing*, sendo necessário a exclusão permanente (não deixar na lixeira);

f. Enviar mensagem com anexos contendo as seguintes extensões .exe, .com, .bat, .pif, .js, .vbs, .hta, .scr, .cpl,*.reg, .dll, .inf* ou qualquer outro arquivo executável que represente um risco à segurança;

g. Veicular publicidade ou propaganda que caracterize concorrência desleal;

h. Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

i. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou suas unidades vulneráveis a ações civis ou criminais;

j. Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

k. Fornecer orientação que conflite ou contrarie os interesses da FNQ;

l. Enviar mensagem que vise a obter acesso não autorizado a outro computador, servidor ou rede;

m. Enviar mensagem que vise acessar informações confidenciais sem explícita e devida autorização;

n. Enviar mensagem que tenha conteúdo considerado impróprio, obsceno ou ilegal;

o. Enviar mensagem que seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

p. Enviar mensagem que contenham perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

q. Enviar mensagem que contenha fins políticos locais ou do país (propaganda política).

2.10. DISPOSITIVOS MÓVEIS E ACESSO REMOTO

Todo colaborador ou parceiro que fizer uso de dispositivos móveis disponibilizados pela FNQ, ou particulares, quando autorizados prévia e expressamente para finalidades profissionais, deve atender às condições estabelecidas na presente política.

Os equipamentos são restritos aos colaboradores previamente autorizados, não sendo permitido o uso de dispositivos móveis disponibilizados pela FNQ por outros colaboradores ou terceiros não autorizados.

O colaborador deve devolver imediatamente e em perfeitas condições de uso e funcionamento o dispositivo móvel corporativo no caso de término de sua contratação ou quando solicitado pela FNQ, independentemente de qualquer motivo.

É vedado o uso de dispositivos móveis particulares para finalidades profissionais, exceto quando previamente autorizado.

Sobre o uso do dispositivo móvel, *Colaboradores* e *Prestadores de Serviço* devem, independentemente se a partir do dispositivo móvel corporativo ou particular autorizado a portar o dispositivo móvel sempre junto a si, ou trancado em ambiente seguro; informar imediatamente os casos de roubo, perda ou furto do dispositivo móvel, notificar imediatamente seu gestor direto, o responsável de TI e procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO); armazenar nos dispositivos móveis corporativos somente arquivos relacionados às atividades profissionais no dispositivo móvel que estiver em sua posse.

Não é permitida a utilização de *software* sem a devida licença para realizar atividades profissionais ou produzir conteúdo para FNQ. Quaisquer danos eventualmente ocorridos no dispositivo móvel corporativo por má utilização do colaborador serão de sua responsabilidade, incluindo os custos decorrentes para a manutenção ou substituição do equipamento

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pelo responsável de tecnologia. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela organização constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É expressamente proibida a captura e divulgação de imagens pelos dispositivos móveis, por qualquer forma, que contenham informações confidenciais, de clientes ou colaboradores.

2.11. HOME OFFICE

É expressamente proibido o uso de equipamentos particulares não autorizados pelo responsável de TI em conexões remotas ao ambiente da FNQ. No caso de dispositivos habilitados e

autorizados para acesso remoto, devem estar configurados pelo responsável de TI, obrigatoriamente, com mecanismos de segurança tais como sistema de criptografia, antivírus, ferramentas para acesso seguro à VPN (*Virtual Private Network*) e *firewall* pessoal, visando assegurar confidencialidade e a integridade das informações. Os serviços remotos deverão ser interrompidos automaticamente após 5 minutos de inatividade, porém, sempre que o colaborador ou parceiro não estiver utilizando os recursos deve encerrar a sua sessão imediatamente.

2.12. *BACKUPS*

O responsável de TI criará as definições e executará os procedimentos e manuais operacionais específicos, conforme as características das informações, dos sistemas e das ferramentas de geração de backup, devendo considerar as seguintes diretrizes: armazenamento seguro e ambientalmente adequado em instalações locais e remotas das mídias, incluindo a eventual geração de backups redundantes como suporte às estratégias de contingência operacional e de continuidade de negócios; utilização de criptografia e restrição de acesso ao material salvaguardado; transporte seguro das mídias que terão armazenamento remoto; descarte seguro de mídias e ferramentas de geração de backups obsoletos, depreciados e danificados, considerando a eliminação definitiva de seu conteúdo e, quando necessário, a destruição do suporte físico.

3. PROTEÇÃO DE DADOS PESSOAIS

Neste documento, como também na *Política de Privacidade* e em documentos específicos da FNQ estarão definidos normas, procedimentos e boas práticas de privacidade e proteção de dados, em especial os dados pessoais nos preâmbulos da LGPD.

3.1. TRATAMENTO DE DADOS E BASES LEGAIS

Durante os processos e atividades diárias para o cumprimento dos objetos contratuais firmados com seus clientes, colaboradores e parceiros inevitavelmente realiza o tratamento de dados destes.

A FNQ e todos seus *Colaboradores* e *Prestadores de Serviço* durante todo o processo de tratamento de dados, observará, em boa fé, todos os princípios e diretrizes da LGPD.

Este tratamento de dados pessoais, fica embasado em obrigações contratuais estabelecidas entre as partes, sejam elas obrigações de cunho comerciais ou administrativas, desta maneira, a FNQ utiliza-se do art. 7º da LGPD com as seguintes *hipóteses legais* para realizar o tratamento de dados:

a. Para **cumprimento de obrigação legal ou regulatória** (Art. 7º, II, da LGPD), em especial quando se tratar à prevenção à corrupção e suborno;

b. Quando necessário para a **execução de contrato** ou de procedimentos preliminares a contrato do qual seja parte o titular de dados pessoais (Art. 7º, V, da LGPD);

c. Para o **exercício regular de direitos** em processo judicial, administrativo ou arbitral (Art. 7º, VI, da LGPD);

d. Quando necessário para atender aos **interesses legítimos do controlador ou de terceiros** (Art. 7º, IX, da LGPD);

e. Para a **proteção do crédito** (Art. 7º, X, da LGPD), incluindo, neste caso, também, a transparência e a precisão nos relatórios financeiros que podem exigir o tratamento de dados pessoais para cumprir, além das obrigações legais e regulatórias e também proteção do crédito;

f. Para o **consentimento** (Art. 7º, I, da LGPD), quando o tratamento de dados pessoais requerer o consentimento do titular, especialmente quando se trata de dados sensíveis ou para finalidades específicas não cobertas por outras bases legais;

g. Para **Proteção da Vida ou da Incolumidade Física** (Art. 7º, VII): Dados de saúde podem ser tratados para proteger a vida e a saúde dos colaboradores, especialmente em situações de emergência ou para garantir um ambiente de trabalho seguro;

h. Quando o tratamento de dados relacionados puder ser justificado pelo interesse legítimo da organização, desde que respeite os direitos e liberdades fundamentais dos titulares, poderá ser utilizado a base do **Interesse Legítimo** (Art. 7º, IX);

Fica definida nesta política que a **FNQ** prioritariamente como controladora de dados pessoais de seus *Colaboradores* e *Prestadores de Serviço,* além de clientes, pode se utilizar de tratamento por terceiros, esses considerado pela LGPD como operadores.

A **FNQ** determina que estes operadores sigam as normativas da LGPD e suas boas práticas, garantido nível similar ao tratamento de dados que a **FNQ** aplica, utilizando obrigatoriamente:

- uma política de privacidade e proteção de dados adequada as suas operações; e
- cláusulas contratuais referentes à proteção de dados pessoais com seus colaboradores e fornecedores.

Sobre a exclusão dos dados pessoais, ocorrerá mediante a solicitação dos titulares e será realizada somente nos casos que não houver nenhum impedimento legal ou necessidade de armazenamento a fim de garantir os direitos da **FNQ**, conforme o Art. 16, I, da LGPD.

3.2. DIREITOS DO TITULAR

Os titulares de dados pessoais têm direito, a qualquer momento, perante às informações armazenadas nas bases de dados da FNQ, de acordo com o Art. 18 da LGPD, requisitar à FNQ, observando a proteção ao direito intelectual:

a. Confirmação da existência de tratamento;
b. Acesso aos dados;
c. Correção de dados incompletos, inexatos ou desatualizados;
d. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta lei;
e. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
f. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da lgpd;
g. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
h. Oposição ao fornecimento do consentimento e sobre as consequências da negativa, quando possível e permitido pela lei;
i. Revogação do consentimento, nos termos do § 5º do art. 8º da lgpd, quando possível e permitido pela lei.

3.3. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os incidentes de segurança da informação serão prevenidos por fiscalização do cumprimento da legislação vigente no Brasil, dos princípios éticos e dos controles estabelecidos pelos normativos da FNQ; monitoramento das vulnerabilidades existentes por meio de ferramentas de supervisão de atividades; registro e análise de trilhas de auditoria e controle de acesso em ambientes físicos e digitais.

Os *Colaboradores* e *Prestadores de Serviço* devem relatar todos os incidentes de segurança da informação que tiver conhecimento imediatamente para o responsável de TI.

Os *Colaboradores* e *Prestadores de Serviço* não devem tomar qualquer ação própria em busca da solução do incidente de segurança da informação, devendo apenas relatá-lo.

Os incidentes de segurança da informação são quantificados e monitorados pelo responsável de TI, a fim de se identificar quais podem ser mais recorrentes ou de maior impacto, além de permitir

implementar ações corretivas e prevenir novas ocorrências.

Após notificação de um incidente de segurança da informação, o responsável de TI toma as ações necessárias para a mitigação de seus impactos e o restabelecimento da condição de normalidade, em seguida notificam a ANPD, se necessário, sobre o fato ocorrido. As ações visam garantir a proteção aos direitos do titular dos dados, a continuidade do negócio da FNQ e de suas atividades, além de realizar o isolamento do ambiente e do dispositivo, caso seja necessário.

Sempre que ocorrerem indícios do envolvimento de um *Colaborador ou Prestador de Serviço* em um incidente de segurança da informação, o responsável de TI pode solicitar o bloqueio de sua identidade digital e demais acessos, além de informar imediatamente aos superiores.

As ações tomadas em resposta a um incidente de segurança da informação são armazenadas de forma organizada e segura com a finalidade de compor uma base de conhecimento para a catalogação das experiências obtidas e análise da eficiência dos controles em vigor e possível auditorias dos órgãos responsáveis.

3.4. ARMAZENAMENTO E DESCARTE DE INFORMAÇÕES FÍSICAS

A FNQ deve cumprir os diferentes prazos que a legislação estabelece para manutenção e guarda de documentos e livros fiscais, físicos e digitais, de acordo com a área correlata ao conteúdo das informações, a exemplo, mas não se limitando a documentos societários, tributários, trabalhistas e previdenciários.

Não é permitido o descarte em lixo comum de documentos confidenciais, como notas fiscais ou cópias impressas de documentos. Estes devem ser triturados em seu descarte físico.

O responsável pela guarda de documentos deve manter o conteúdo organizado, em bom estado e de rápido acesso aos colaboradores e parceiros autorizados, sempre que necessário.

Da mesma forma, deve avaliar o estado físico da documentação, o volume a ser guardado e transferir toda documentação inativa ou não mais necessária para arquivo físico local ou terceirizado.

A guarda dos documentos deve ser organizada, sigilosa, segura (sem fonte de ignição para incêndio) e com movimentação restrita a colaboradores previamente autorizados.

3.5. TREINAMENTO

A FNQ preza pela excelência da execução de suas atividades, sendo a segurança e proteção de dados uma delas, desta forma ela se compromete que seus colaboradores e parceiros passem por treinamentos adequados e periódicos em boas práticas de segurança da informação de proteção de dados pessoais.

Desta maneira fica determinada nesta política, treinamentos, no mínimo, anuais de LGPD e *Cyber Awareness*, além da integração de novos colaboradores e parceiros

Estes treinamentos são adotados como obrigatórios e sempre serão ministrados por profissionais capacitados com certificações que comprovem os conhecimentos sobre o assunto.

4. OUTRAS DISPOSIÇÕES

A seguir serão tratadas políticas que abordam certos aspectos e requisitos da FNQ.

4.1. IDENTIFICAÇÃO VISUAL

O uso do crachá de identificação, quando o trabalho for presencial, é obrigatório, pessoal e intransferível para todos os colaboradores e parceiros. Deverá ser portado em lugar bem visível durante todo o tempo de permanência e no exercício do trabalho.

Quando executar serviços externos, o crachá também deverá ser utilizado, sendo seu uso imprescindível para segurança do ambiente de trabalho e identificação correta de seu portador. Em caso de perda, um novo crachá deve ser requisitado imediatamente ao Departamento de RH. FNQ.

4.2. CARTÃO DE ACESSO

A FNQ disponibilizará aos seus colaboradores e parceiros um cartão para controle de acesso, quando necessário a realização de trabalho nas suas dependências físicas. Este cartão é intransferível e de uso somente do portador, ficando vedado seu empréstimo a outro colaborador ou terceiro.

O controle de acesso, quando utilizado, retém *logs* sendo possível a realização de auditoria pela FNQ.

4.3. CERTIFICADO DIGiTAL

É *vedado* ao colaborador ou parceiro confiar a guarda ou compartilhar o certificado digital da FNQ a terceiros, como também fazer uso de certificados digitais de terceiros sem a devida procuração e autorização deste.

É *terminantemente proibido* ao colaborador ou parceiro utilizar certificado digital de clientes, seja qual for a mídia ou nível de segurança.

É *vedado* ao colaborador ou parceiro utilizar seu certificado e-CPF, caso possua, para realizar trabalhos profissionais, devendo este deve ser mantido em sua posse.

Caso alguma das atividades exija a utilização do certificado digital do cliente e que não seja possível a utilização de procuração, deve-se solicitar ao cliente seu compareçimento presencial, portando o certificado, para viabilizar a realização da mesma.

Quanto ao procedimento para outorgar e revogar procuração, o colaborador autorizado da FNQ deverá comparecer na empresa do cliente para as devidas orientações com finalidade de realizar as procurações, dentre elas:

- Receita Federal/Procuradoria Geral da Fazenda Nacional, Secretaria da Fazenda e Procuradoria Estadual, Caixa Econômica Federal/Conectividade Social.

Os dispositivos de identificação e senhas, incluindo os certificados digitais, protegem a identidade dos *Colaboradores* e *Prestadores de Serviço*, evitando e prevenindo fraudes perante a FNQ e/ou terceiros.

Desta forma, o uso dos dispositivos de segurança, incluindo certificados digitais e/ou senhas de identificação de outra pessoa, constitui crime tipificado no Código Penal Brasileiro (art. 307 - falsa identidade).

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação vigente (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal não poderá ser compartilhado com outras pessoas em nenhuma hipótese. Em caso de não observância de tal regra, a responsabilidade perante a FNQ e a legislação vigente (cível e criminal) será dos usuários que dele se utilizarem.

4.4. MONITORAÇÃO E INSPEÇÃO

Os *Colaboradores* e *Prestadores de Serviço* estão cientes de que a FNQ realiza o registro e armazenamento de atividades (*logs*), monitorando todo acesso e uso de seus ambientes físicos e digitais com a captura de imagens, áudio ou vídeo, inclusive, com a finalidade de proteção de seu patrimônio e reputação e daqueles com quem se relaciona, de alguma forma, além de colaborar com as autoridades em caso de investigação.

Sempre que considerar necessário, a FNQ pode auditar ou inspecionar os recursos de tecnologia que interagem com seus ambientes físicos ou digitais ou com suas informações, quando autorizada a entrada em suas dependências.

4.5. IMPRESSÃO

O serviço de impressão destina-se *exclusivamente* às atividades de cunho empresarial da FNQ. A sustentabilidade ambiental é elemento chave na utilização do serviço - a impressão de documentos deve ser evitada sempre que possível.

Deve-se buscar a tramitação de processos administrativos sempre na forma eletrônica, fazendo uso da impressão apenas nos casos em que se requer assinatura ou carimbos impressos ou que seja um pré-requisito.

Deve-se evitar impressão de qualquer dado pessoal conforme informado elencado na LGPD.

Ao imprimir qualquer documento o colaborador ou parceiro deverão ser adotados todos os cuidados de segurança necessários para que nenhuma pessoa sem autorização tenha acessa a dados confidenciais e/ou pessoais de qualquer cliente, colaborador e/ou fornecedor da FNQ.

Todo e qualquer impresso que já cumpriu sua necessidade deve ser fragmentado por meio hábil e autorizado pela FNQ.

4.6. MESA LIMPA e TELA LIMPA

A FNQ adota ações como padrão para assegurar a proteção da integridade, confidencialidade e disponibilidade (*Triadi Cid*) de dados e informações sensíveis, através da Política da *Mesa Limpa,* visando minimizar os riscos associados ao acesso não autorizado, perda, alteração ou destruição de informações confidenciais durante ou fora do expediente, sendo obrigatório a todos os *Colaboradores* e *Prestadores de Serviço:*

a. Manter a mesa organizada;

b. Guardar qualquer documento que possa conter dados pessoais ou estratégicos da FNQ e de seus clientes;

c. Não deixar exposto informações estratégicas, dados pessoais e senhas em papeis colados em sua mesa;

d. Anotações, post-its e outros materiais que possam conter informações sensíveis devem ser descartados de maneira adequada, utilizando trituradores de papel quando necessário.

e. Recolher papeis e documentos da sua mesa, eliminando aqueles que não possuem mais uso.

f. Ao final do expediente, os colaboradores devem garantir que não haja documentos deixados sobre mesas, impressoras ou áreas comuns.

g. Computadores e outros dispositivos eletrônicos devem ser bloqueados ou desligados quando não estiverem em uso, especialmente ao se afastar da estação de trabalho.

h. Dispositivos portáteis, como laptops e tablets, devem ser guardados em locais seguros quando não estão sendo utilizados.

Para manutenção dos padrões mínimos de segurança de informação junto à FNQ, a Política da *Mesa Limpa* deverá ser observada *inclusive* quando o trabalho ocorrer em homeoffice, coworking, viagens, escritórios de clientes e parceiros.

a. **ACESSO A ÁREAS RESTRITAS:** O acesso a áreas onde informações sensíveis são processadas ou armazenadas deve ser restrito apenas ao pessoal autorizado.

A implementação desta política é essencial para garantir que todos os *Colaboradores* e *Prestadores de Serviço* contribuam para um ambiente de trabalho seguro e em conformidade com as normas de proteção de dados e boas práticas.

5. PAPÉIS E RESPONSABILIDADES

Além das funções e tarefas, serão elencadas a seguir as responsabilidades dos envolvidos na política da segurança da informação e proteção de dados da FNQ.

a. Diretores e gestores:

- Observar as diretrizes e normas previstas no Estatuto, aprovar os normativos da FNQ, orientar e acompanhar o estabelecimento e a observância dos controles estabelecidos, além de analisar as questões específicas apresentadas pelos *Colaboradores* e *Prestadores de Serviço,*.

b. Responsável de TI:

- Definir os requisitos e controles adequados para a proteção das informações e recursos tecnológicos da FNQ;
- Avaliar periodicamente os sistemas e equipamentos, com o intuito de verificar o cumprimento dos normativos;
- Implementar os controles de segurança previstos nesta norma para proteção das informações e dos recursos tecnológicos;
- Manter os softwares de proteção instalados, ativos e atualizados;
- Adquirir, de acordo com o orçamento da FNQ, recursos tecnológicos quando autorizado pela Diretoria;
- Tomar as medidas cabíveis em caso de perda, furto ou roubo de qualquer recurso tecnológico da FNQ;
- Proceder com a manutenção, instalação, análise, configuração ou remanejamento de quaisquer recursos tecnológicos;
- Estabelecer mecanismos de identificação e autenticação de forma que possibilite a rastreabilidade das atividades do colaborador ou parceiro;

Rua irmã Gabriela, 51, Cidade Monções
CEP: 04571-130 • São Paulo/SP
Telefone: +55 (11) 5509-7700

www.fnq.org.br

- Fornecer a senha ao colaborador ou parceiro de forma segura, sigilosa e de maneira que a sua alteração seja exigida no primeiro acesso;
- Auxiliar no processo de revisão de acessos concedidos; conceder, ajustar ou revogar o acesso do colaborador ou parceiro, quando solicitado formalmente ou em caso de encerramento das atividades;
- Realizar e testar o *backup* das informações e recursos tecnológicos críticos para a FNQ;
- Realizar o monitoramento e manter o valor probatório dos registros para fins legais, preservando a confidencialidade, integridade, autenticidade, legalidade e disponibilidade das informações.

c. Responsável do RH:

- Auxiliar na promoção da divulgação e capacitação sobre segurança de informação na FNQ;
- Autorizar, ou não, a concessão de acesso solicitada pelo gestor do colaborador;
- Comunicar formal e imediatamente qualquer admissão, alteração de cargo ou atividade dos colaboradores para o responsável de TI, para que este crie ou altere as contas de acesso correspondentes;
- Realizar a revisão dos acessos concedidos, no mínimo a cada 6 meses, em conjunto com o responsável de TI;
- Informar o encerramento das atividades, férias, licenças e ausência temporária dos colaboradores ao responsável de TI, imediatamente.

d. Responsável pelas questões jurídicas:

- Agir, sempre que acionado pelo pela Diretoria, nos casos de incidente de segurança da informação que possam envolver processos jurídicos;
- Elaborar uma tabela de temporalidade de modo a garantir o armazenamento e o descarte das informações de acordo com os prazos estabelecidos pela legislação nacional vigente;
- Auxiliar nas adequações necessárias aos contratos de clientes, fornecedores e colaboradores

e. Gestor responsável pelo *Colaboradores* e *Prestadores de Serviço*:

- Orientar constantemente suas equipes quanto ao uso ético, seguro e de acordo com a legislação nacional vigente dos ativos tangíveis e intangíveis da FNQ;

- Autorizar, ou não, o uso de dispositivos móveis corporativos ou particulares pelos colaboradores supervisionados;
- Assegurar o cumprimento desta norma por parte dos colaboradores supervisionados;
- Participar da investigação de incidentes de segurança relacionados às informações, recursos de TI e colaboradores sob sua responsabilidade.

f. *Colaboradores* e *Prestadores de Serviço*:

- Cumprir e manter-se atualizado em relação à esta política; utilizar de forma ética, segura e de acordo com a legislação nacional vigente todos os ativos corporativos, respeitando os direitos e as permissões de uso concedidas pela FNQ;
- Zelar para que todas as informações inseridas nos recursos tecnológicos, ou quando enviadas ao cliente, sejam necessárias, livres de erro, transparentes e verídicas;
- Utilizar as informações e os recursos tecnológicos da FNQ somente para finalidades profissionais e restritas as atividades contratadas;
- Classificar e rotular todas as informações confidenciais no momento da sua criação ou recebimento;
- Tratar a senha de forma individual, sigilosa e intransferível, não compartilhando ou divulgando a terceiros;
- Triturar as informações físicas, sempre que necessário o seu descarte;
- Reportar imediata e formalmente qualquer caso comprovado, passível de comprovação ou cuja suspeita seja fundamentada de descumprimento desta política ou de qualquer incidente de segurança da informação, sob pena de sua conduta ser considerada omissa, negligente ou conivente;
- Atuar de forma transparente, evitando toda forma de corrupção, fraude, suborno, favorecimento, extorsão, benefícios e vantagens.

g. Encarregado de dados:

O Encarregado de Dados desempenha um papel crucial na gestão da proteção de dados dentro da FNQ. Suas principais funções incluem:

- Atuar como ponto de contato para os titulares de dados, respondendo a consultas, solicitações e queixas relacionadas ao tratamento de dados pessoais.
- Monitorar e assegurar que a FNQ esteja em conformidade com a LGPD e outras regulamentações de proteção de dados aplicáveis.

Rua irmã Gabriela, 51, Cidade Monções
CEP: 04571-130 • São Paulo/SP
Telefone: +55 (11) 5509-7700

www.fnq.org.br

- Aceitar reclamações, comunicações e solicitações dos titulares de dados, prestar esclarecimentos e adotar providências;
- Promover a conscientização e o treinamento contínuo dos colaboradores sobre práticas de proteção de dados e privacidade
- Receber comunicações da autoridade nacional e adotar providências; orientar os colaboradores e os contratados da FNQ a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Coordenar e supervisionar a realização de avaliações de impacto à proteção de dados, quando necessário, para identificar e mitigar riscos associados ao tratamento de dados pessoais.
- Reportar regularmente à alta administração sobre o status da conformidade com a LGPD e quaisquer riscos ou incidentes relacionados à proteção de dados.

h. Comitê de Segurança e Privacidade de Dados:

- Trabalhar em estreita colaboração com o Encarregado de Dados para garantir uma abordagem integrada à proteção de dados e à segurança da informação;
- Aprovar e revisar anualmente, ou sempre que se faça necessário, o processo de gestão de riscos de tecnologia, de acordo com as boas práticas mundialmente reconhecidas;
- Aprovar e revisar anualmente, ou sempre que se faça necessário, a política de segurança da informação, o processo de segurança da informação e o processo de gerenciamento de incidentes de segurança da informação em harmonia com as diretrizes nacionais, bem como as boas práticas de segurança da informação mundialmente reconhecidas;
- Analisar e responder a incidentes de segurança e violações de dados, garantindo que ações corretivas sejam implementadas e que lições sejam aprendidas.
- Estabelecer no âmbito institucional uma cultura de boas práticas voltada para segurança da informação;
- Definir os serviços de tecnologia considerados críticos para a FNQ;
- Definir investimentos em segurança da informação, com base em relatórios de gestão de riscos e pesquisas de mercado;
- Fornecer relatórios regulares à direção sobre questões de segurança e privacidade, incluindo recomendações para melhorias;
- Definir o risco de tecnologia da FNQ em harmonia com as boas práticas de segurança da informação mundialmente reconhecidas.

6. PROCESSO DISCIPLINAR

Os *Colaboradores* e *Prestadores de Serviço* que tomarem atitudes antiéticas, ilícitas, não autorizadas ou contrárias ao recomendado pela FNQ e consideradas violações por si só, estão sujeitos às sanções cabíveis, podendo variar desde advertência verbal ou escrita, até a rescisão do contrato por justa causa.

A tentativa de burlar as diretrizes e controles estabelecidos deve ser desestimulada e, quando constatada, será tratada como violação às normas da empresa.

Atos de desonestidade, incontinência de conduta ou mau procedimento, negociação habitual por conta própria ou alheia sem permissão, concorrência desleal, desídia, embriaguez habitual ou em serviço, violação de segredo da empresa, indisciplina ou insubordinação, abandono de emprego, lesão contra a honra ou boa fama de qualquer pessoa ou ofensas físicas nas mesmas condições e prática de jogos de azar, enquadrados no art. 482 da Consolidação das Leis do Trabalho - CLT, ao ocorrerem serão punidos com demissão por justa causa, obedecendo os preceitos legais.

No caso de parceiros que prestam serviços para FNQ, terão as rescisões contratuais solicitadas de forma forçada por descumprimento da política ora mencionada.

Para a apuração dos fatos internamente, será instaurado o devido *Processo Interno Displinar*, conforme abaixo descrito, através dos procedimentos autorizados pelo Estatudo e legislação pernitente, assegurando ao investigado o contraditório e ampla defesa, na forma da Lei.

a. Recebimento da Denúncia ou Identificação da Conduta

- Coleta de Informações: O processo inicia-se com o recebimento de uma denúncia formal ou a identificação de uma possível infração às normas internas. As denúncias podem ser feitas por colaboradores, terceiros ou através de canais de denúncia anônimos.
- Registro Formal: A denúncia deve ser registrada formalmente, detalhando a natureza da acusação, as partes envolvidas e quaisquer evidências preliminares disponíveis.

b. Análise Preliminar

- Avaliação Inicial: Uma análise preliminar é conduzida para determinar a veracidade e a gravidade da denúncia. Nesta fase, decide-se se há fundamento suficiente para prosseguir com uma investigação formal.
- Decisão de Prosseguir: Caso a análise preliminar indique a necessidade de investigação, um processo formal é instaurado.

c. Instauração do Processo Disciplinar

- Nomeação de Comissão: Uma comissão de investigação é nomeada, composta por membros imparciais e qualificados para conduzir a investigação de forma justa e objetiva.

- **Notificação das Partes:** As partes envolvidas são notificadas sobre a instauração do processo, sendo informadas sobre seus direitos e deveres durante a investigação.

d. Investigação Formal

- **Coleta de Evidências:** A comissão coleta todas as evidências relevantes, incluindo documentos, registros eletrônicos, depoimentos de testemunhas e quaisquer outras informações pertinentes.
- **Entrevistas:** As partes envolvidas, incluindo o acusado e testemunhas, são entrevistadas para obter suas versões dos fatos.
- **Análise de Evidências:** A comissão analisa todas as evidências coletadas para determinar a ocorrência de violações das normas e regulamentos internos.

e. Conclusão da Investigação

- **Elaboração do Relatório:** A comissão elabora um relatório detalhado com as conclusões da investigação, incluindo as evidências analisadas e recomendações sobre as medidas disciplinares a serem adotadas, se necessário.
- **Revisão e Aprovação:** O relatório é revisado por instâncias superiores ou pelo departamento jurídico para garantir conformidade com as políticas internas e legais.

f. Decisão e Aplicação de Medidas Disciplinares

- **Decisão Final:** Com base no relatório da comissão, a administração da **FNQ** toma uma decisão final sobre o caso, determinando as medidas disciplinares a serem aplicadas, que podem variar de advertências a demissões, dependendo da gravidade da infração.
- **Notificação:** As partes envolvidas são notificadas da decisão final e das medidas disciplinares aplicadas.

g. Encerramento do Processo

- **Registro e Arquivamento:** Todos os documentos e registros relacionados ao processo disciplinar são arquivados de forma segura e confidencial, para referência futura e conformidade com requisitos legais.
- **Feedback e Melhoria Contínua:** Lições aprendidas durante o processo são analisadas para melhorar políticas e procedimentos internos, prevenindo futuras ocorrências.

7. DISPOSIÇÕES FINAIS

Este Código de Conduta e Segurança encontra-se disponível na pasta de rede e será enviada para todas as partes envolvidas nas atividades da **FNQ**; deverá ser disponibilizada na contratação de *Colaboradores* e *Prestadores de Serviço* e estar disponível para os titulares de dados sempre que

necessário, ou em caso de indisponibilidade, pode ser solicitada para o encarregado de dados.

Em caso de dúvidas, *Colaboradores* e *Prestadores de Serviço* podem solicitar os esclarecimentos necessários por meio do e-mail ao encarregado de dados da FNQ.

Ainda, esta política deve ser revista e atualizada em intervalos não superiores a dois anos, visando a garantir que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente no Brasil.

8. DA APROVAÇÃO

Este documento foi redigido por *Ana Cláudia Ferigato – Ana Ferigato Consultoria em LGPD*, tendo sido devidamente apresentado e aprovado pela FNQ em agosto de 2024.

A. Glossário de termos.

Para efeitos de entendimento e fácil compreensão da política criada, serão apresentados as definições legais e conceitos que são utilizados neste documento.

i. FNQ – Fundação Nacional da Qualidade.

ii. **Dados:** parte da estrutura incapaz de gerar conclusões inteligíveis, mas computáveis. Representa uma ação não descrita, uma quantidade sem especificar o objeto.

iii. **Dados pessoais:** todos os tipos de dados que podem levar à identificação de uma pessoa, de forma direta ou indireta. Alguns tipos de dados pessoais incluem (nome completo, RG, CPF, endereço, telefone, e-mail, endereço de IP, data de nascimento, entre outros).

iv. **Dados sensíveis:** Qualquer informação que relacione com a origem racial, étnica, credo, opinião política, filiação a sindicato; que se referem à saúde ou vida sexual, dados genéticos e biométricos.

v. **Dados anonimizados:** operação que seja realizada com os dados pessoais de forma anônima, sem que haja identificação do indivíduo.

vi. **Dados públicos:** dados que ainda públicos podem ser restringidos pelo indivíduo.

vii. ANPD - Autoridade Nacional de Proteção de Dados: órgão da administração pública direta federal com atribuições relacionadas à regulamentação e fiscalização do cumprimento da LGPD.

viii. Titular: pessoa a quem se referem os dados pessoais que são objeto de tratamento.

ix. Controlador: pessoa física ou jurídica, a quem competem as decisões referentes ao tratamento de dados pessoais.

x. Operador: pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

xi. **Encarregado de dados:** responsável frente à ANPD e aos titulares indicados pelo controlador.

xii. **Tratamento de dados:** qualquer operação que seja realizada com os dados pessoais (incluindo: acesso, armazenamento, arquivamento, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração, modificação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização).

xiii. Cliente: pessoa física ou jurídica que contrate os serviços da empresa.

xiv. Colaborador: pessoa que faz parte do quadro de contratados.

xv. **Parceiro/prestador:** pessoa física ou jurídica que presta serviços no âmbito das atividades.

xvi. Recursos tecnológicos: todos os recursos físicos e digitais utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar informações. Entre os tipos de recursos podemos destacar: computadores de mesa ou portáteis, *smartphones*, *tablets, pen drives*, discos externos, mídias, impressoras, *scanner*, entre outros.

xvii. **Dispositivo móvel:** qualquer equipamento eletrônico com atribuições de mobilidade.

xviii. **Incidentes de segurança da informação:** ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação a esta política, a LGPD, falha de controles, ou situação previamente desconhecida, que possa ser relevante à segurança da informação. São exemplos de Incidentes de Segurança da Informação: perda de serviços ou recurso; mau funcionamento ou sobrecarga de sistema; erros humanos; não conformidade, observações ou suspeitas de fragilidade em sistemas ou serviços; vazamento de informação de clientes ou pessoas que estejam armazenadas e tratadas em no ambiente digital; violações de procedimentos de segurança e violações de acesso.

xix. **Evasão de Segurança:** ações ou técnicas utilizadas para contornar ou burlar medidas de segurança implementadas em sistemas de informação.

xx. **Exploração de Vulnerabilidades:** Utilizar falhas ou bugs em software ou hardware para obter acesso não autorizado a sistemas.

xxi. **Engenharia Social:** Manipular indivíduos para que divulguem informações confidenciais ou realizem ações que comprometam a segurança, como clicar em links maliciosos ou fornecer credenciais de acesso.

xxii. **Endereço IP:** Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255, por exemplo, "192.0.2.2".

xxiii. **Firewall:** Dispositivo de segurança usado para dividir (*conhecido como muro*) e controlar o acesso entre redes de computadores.

xxiv. **Ataques de Phishing:** Enviar comunicações fraudulentas que parecem ser de fontes confiáveis para enganar os destinatários e obter informações sensíveis.

xxv. **Malware**: Implantar software malicioso em sistemas para roubar dados, danificar sistemas ou realizar outras atividades prejudiciais.

xxvi. **Cavalo de Tróia:** um programa que além de executar as funções para as quais foi aparentemente projetado também executa outras funções, normalmente maliciosas, sem o conhecimento do usuário, tais como, furto de senhas, de números de cartões de crédito e outras informações pessoais e, também, inclusão de backdoors.

xxvii. **Conexão segura:** Conexão que utiliza um protocolo de criptografia para a transmissão de dados, como por exemplo, HTTPS ou SSH.

xxviii. **Bypass de Autenticação:** Contornar mecanismos de autenticação, como senhas ou autenticação de dois fatores, para acessar sistemas de forma não autorizada.

xxix. **Interceptação de Comunicação:** Capturar dados transmitidos entre sistemas, como em ataques "*man-in-the-middle*", para acessar informações confidenciais.

xxx. **LGPD** - Lei Geral de Proteção de Dados Pessoais, Lei de nº 13.709/2018 que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa física ou jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade.

xxxi. **Criptografia:** conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

xxxii. **VPN:** Uma Rede Privada Virtual (VPN, do inglês *Virtual Private Network*) é uma tecnologia que cria uma conexão segura e criptografada sobre uma rede menos segura, como a Internet.

xxxiii. **Compliance:** O termo deriva da palavra inglesa "*to comply*" e significa estar em conformidade. Na prática, o termo tem a função de proporcionar segurança e minimizar riscos de instituições e empresas, garantindo o cumprimento dos atos, regimentos, normas e leis estabelecidos interna e externamente.

xxxiv. **Due Dilligence:** Investigação analítica e detalhada da situação de uma empresa, instituição ou projeto. Tem como objetivo principal a identificação de passivos que possam vir a causar impactos negativos nos âmbitos da instituição que a contrata.

xxxv. **Pessoas Politicamente Expostas (PEP):** Agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou em países, territórios e dependências estrangeiras, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e estreitos relacionamentos dos participantes.

xxxvi. **Assédio:** O assédio refere-se a comportamentos indesejados e repetitivos que têm como objetivo ou efeito criar um ambiente intimidador, hostil, degradante, humilhante ou ofensivo para a vítima. O assédio pode ocorrer em várias formas, incluindo, mas não se limitando ao assédio Moram, sexual ou racial.

xxxvii. **Assédio Sexual:** Comportamentos de natureza sexual que são indesejados e ofensivos para a vítima. Exemplos incluem comentários sexuais, avanços sexuais não desejados, toques inapropriados, entre outros.

xxxviii. **Assédio Moral:** Comportamentos que visam humilhar, ridicularizar, ou desestabilizar emocionalmente a vítima. Exemplos incluem insultos, críticas constantes, isolamento social no ambiente de trabalho etc.

xxxix. **Assédio Racial:** Comportamentos que discriminam ou ofendem alguém com base em sua raça ou etnia. Exemplos incluem piadas racistas, exclusão baseada na raça etc.