Conselho Federal de Química

Plenário
Presidência
Gabinete

PORTARIA Nº 87, DE 9 DE AGOSTO DE 2024

Estabelece diretrizes de segurança da informação para a política de controle de acesso do Conselho Federal de Química.

O PRESIDENTE DO CONSELHO FEDERAL DE QUÍMICA (CFQ), no uso das atribuições que lhe foram conferidas pelos incisos II e XXVI do art. 74 da Resolução Normativa CFQ Nº 307, de 22 de março de 2023;

Considerando a Instrução Normativa GSI/PR N° 01, de 27 de maio de 2020 que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Considerando a ABNT NBR ISO/IEC 27002: 2013 que contém o código de Prática para controles de Segurança da Informação;

Considerando a Lei n° 13.709/2018 que dispõe sobre a Lei Geral de Proteção de Dados;

Considerando o CIS v8 - Center for Internet Security (CIS);

Considerando o Guia do Framework de Privacidade e Segurança da Informação elaborado pela Secretaria de Governo Digital do Ministério da gestão e da Inovação em Serviços Públicos;

Considerando o Modelo para Política de Controle de Acesso elaborado pela Secretaria de Governo Digital do Ministério da gestão e da Inovação em Serviços Públicos;

Considerando a Portaria CFQ nº 182 de 6 de outubro de 2022 que dispõe sobre a institucionalização da Política de Segurança da Informação (POSIN) no âmbito do Conselho Federal de Química (CFQ) e dá outras providências;

Resolve:

Art. 1º Aprovar, no âmbito do Conselho Federal de Química - (CFQ), a Política de Uso e Acesso à Internet, em complemento às diretrizes estabelecidas no Capítulo II, na Seção V, Subseção II, da Política de Segurança da Informação, institucionalizada na Portaria CFQ nº 182, de 6 de outubro de 2022.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Seção I

Regras gerais para uso de internet

Art. 2º O acesso à internet fornecido aos usuários da infraestrutura de rede do CFQ deve ser utilizado exclusivamente para atender aos interesses e necessidades institucionais do Conselho.

Art. 3º O uso da internet pelos usuários da rede deverá observar a ética, integridade, licitude, bom senso e a razoabilidade.

Art. 4º É atribuição exclusiva da Gerência de Tecnologia da Informação - GETIC definir os padrões de softwares homologados para uso da internet no CFQ, bem como a forma de

identificação dos usuários e o monitoramento e gestão de tráfego de rede..

Seção II

Conceitos e definições

Art. 5º Para efeitos desta Política, serão considerados os conceitos e as definições de segurança da informação estabelecidos pela Portaria GSI/PR N° 93, de 18 de outubro de 2021 , que aprova o Glossário de Segurança da Informação, adotado pela Política de Segurança da Informação do CFQ, institucionalizada na Portaria CFQ nº 182, de 6 de outubro de 2022, destacando-se:

I. ativo de rede - equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores;

II. ativos de informação - os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

III. bom senso - refere-se à aplicação de princípios práticos e razoáveis ao tomar decisões relacionadas à segurança. Isso envolve o uso do julgamento prudente para avaliar situações específicas, considerar os interesses das partes envolvidas e implementar medidas proporcionais e eficazes. O bom senso ajuda a evitar respostas excessivas ou desproporcionais aos riscos de segurança;

IV. browser - programa criado para permitir a navegação pela internet; sinônimo, em inglês, para navegador de internet;

V. central de serviços - ferramenta de abertura de chamados técnicos de TIC do CFQ;

VI. certificado digital - conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave criptográfica e uma pessoa física, jurídica, máquina ou aplicação;

VII. códigos maliciosos - são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador (do inglês *malware*);

VIII. incidente - evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

IX. incidente de segurança - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

X. informação classificada - informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada conforme procedimentos específicos de classificação estabelecidos na legislação vigente;

XI. informação pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

XII. informação sigilosa - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo;

XIII. infraestrutura de rede - composta pela rede de computadores e todos os sistemas CFQ que se encontram ou que vierem a ser homologados pela GETIC;

XIV. internet - rede global composta pela interligação de inúmeras redes, que conecta mais de 500 milhões de usuários, provendo comunicação e informações das mais variadas áreas de conhecimento;

XV. licitude - refere-se à conformidade com a lei. Em uma política de segurança, a licitude implica que todas as ações e medidas adotadas devem estar em estrita conformidade com as leis, regulamentos e normas pertinentes. Isso garante que todas as práticas de segurança sejam legalmente justificáveis e não infrinjam os direitos ou liberdades dos indivíduos;

XVI. *peer-to-peer* - do inglês par-a-par ou simplesmente ponto-a-ponto, com sigla P2P é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central;

XVII. proxy - servidor que atende a requisições repassando os dados a outros servidores ou requisitantes. Dentre suas inúmeras funções, no quesito segurança, o proxy é usado como filtro de conteúdo, impedindo o acesso a conteúdo proibido pela política de segurança da organização;

XVIII. razoabilidade - implica que as medidas de segurança adotadas devem ser justificáveis e proporcionais à ameaça ou risco percebido, significando que as restrições impostas e as práticas de segurança implementadas devem ser razoáveis em relação aos benefícios esperados em termos de proteção e mitigação de riscos;

XIX. rede de computadores - conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

XX. rede local CFQ - grupo de computadores e dispositivos periféricos que compartilham uma linha de comunicação comum ou link sem fio com um ou mais servidores dentro do espaço físico do CFQ;

XXI. rede de acesso público à Internet: Infraestrutura de rede disponibilizada pelo CFQ que permite o acesso à internet a seus usuários, incluindo visitantes e pessoas sem vínculo formal com a instituição, conforme as diretrizes e políticas estabelecidas;

XXII. redes sociais - estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns;

XXIII. reputação de URL - sistema de classificação de reputação que coleta dados de segurança de dezenas de milhões de sensores localizados em diversos países. Esse sistema utiliza uma tecnologia que analisa padrões de tráfego e vinculações, comportamentos de sites, análise de conteúdo e hospedagem e registro de sites para desenvolver uma classificação de reputação geral para o site. Esse sistema é atualizado automaticamente e frequentemente.

XXIV. vírus - seção oculta e auto-replicante de um software de computador, geralmente utilizando lógica maliciosa, que se propaga pela infecção (isto é, inserindo uma cópia sua e se tornando parte) de outro programa; não pode se auto-executar, ou seja, necessita que o seu programa hospedeiro seja executado para se tornar ativo;

XXV. virtual private network (VPN) - refere-se à construção de uma rede privada utilizando redes públicas (por exemplo, a internet) como infraestrutura; esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado seja interceptado enquanto estiver passando pela rede pública;

XXVI. vulnerabilidade - conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação, e;

XXVII. usuário - pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da assinatura de Termo de Responsabilidade.

Seção III
Permissão de acesso à internet

Art. 6º Todos os usuários da rede local e visitantes do CFQ têm o direito de acessar a internet, de acordo com as regras estabelecidas nesta Política.

Seção IV
Cancelamento e bloqueio do acesso à internet

Art. 7º O acesso à internet pelo usuário da rede local será cancelado quando do seu desligamento da Instituição, ao final do contrato ou de qualquer outro ato jurídico que mantenha vínculo com o Conselho.

Art. 8º O cancelamento, o bloqueio e o desbloqueio do acesso à internet seguem as orientações previstas na Política de Segurança da Informação - POSIN do CFQ.

Seção V

Uso da internet

Art. 9º O acesso à internet na rede do CFQ é concedido de forma pessoal e intransferível, sendo o usuário o único e total responsável por suas ações e por eventuais danos causados ao Conselho e a terceiros.

Art. 10. O acesso à internet, quando realizado pela rede local disponibilizada pela GETIC por meio do browser homologado e disponibilizado nas estações de trabalho do CFQ ou equipamentos portáteis, não poderá ser feito por softwares ou dispositivos que permitam burlar as regras de acesso estabelecidas.

Art. 11. O usuário da rede deverá utilizar a internet de forma a não causar tráfego desnecessário na rede local do CFQ.

Art. 12. A GETIC decidirá sobre os serviços disponibilizados via internet que serão acessados via rede local do CFQ, após a avaliação e emissão de relatório técnico, que deverá considerar os aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

Seção VI

Vedações na utilização da internet

Art. 13. É vedado:

I. acessar sites com códigos maliciosos e vírus de computador;

II. acessar sites com materiais e conteúdos inapropriados, tais como: ofensivos, obscenos, pornográficos, sexualmente sugestivos, abusivos, discriminatórios, difamatórios, ameaçadores e de ódio;

III. acessar sites que infrinjam a Lei nº 7.716, de 5 de janeiro de 1989, que define os crimes resultantes de preconceito de raça ou de cor;

IV. acessar sites que infrinjam as leis de propriedade intelectual;

V. acessar sites que infrinjam as leis de privacidade;

VI. acessar sites ou quaisquer aplicações com finalidades comerciais ou particulares;

VII. realizar download de arquivos que não estejam relacionados às necessidades das atividades desempenhadas no CFQ, em especial, arquivos que contenham materiais ilegais ou que não respeitem os direitos autorais;

VIII. utilizar programas de downloads do tipo P2P (*Peer-to-peer*);

IX. acessar jogos online, exceto nos casos em que tais ações sejam condizentes com atividades desempenhadas no CFQ;

X. assistir a programas, a filmes, a vídeos e a séries, independentemente do canal no qual estejam veiculados, exceto nos casos em que tais ações sejam condizentes com as atividades desempenhadas no CFQ;

XI. disponibilizar informações de propriedade ou custodiadas pelo CFQ na internet, sem prévia autorização do responsável pela respectiva informação;

XII. utilizar a internet fornecida pelo CFQ para mineração de moedas virtuais;

XIII. passar-se por outra pessoa ou dissimular sua identidade quando utilizar os recursos da internet;

XIV. utilizar programas e dispositivos para burlar os controles estipulados nesta Portaria; e

XV. instalar e/ou acessar, seja remoto ou local, aos programas e sítios de relacionamento, mídias sociais (sites) e/ou comunicação de qualquer espécie, onde se incluem, mas não exclusivamente, *“Twitter”, “Facebook”, “linkedin”, “Instagram”, “Badoo”, “Youtube”, “Vimeo”, “TeamViewer”* e outros, que não os mantidos ou administrados pelo próprio CFQ, se houverem, ou quando expressamente autorizados a bem das atividades desempenhadas no CFQ.

Parágrafo único. O descumprimento das vedações previstas neste artigo serão apuradas de acordo com a POSIN e o código de ética do CFQ.

Seção VII

Outras vedações e/ou liberações

Art. 14. O usuário sempre deverá certificar-se da procedência do site, verificando, quando cabível, o certificado digital do mesmo, principalmente para realizar transações eletrônicas via internet, digitando o endereço do site diretamente no browser da estação de trabalho, nunca

clicando em um link existente em uma página ou em uma mensagem de correio eletrônico desconhecidas ou pouco confiáveis.

Art. 15. É vedado aos usuários disponibilizar informações de propriedade do CFQ em sites da internet sem observar sua classificação e o público a que se destina.

Art. 16. Serão instituídos grupos de acesso com objetivo de possibilitar maior controle, disponibilidade, desempenho e segurança do serviço de Internet, com bloqueios a diferentes categorias de URL.

Art. 17.As categorias de URL's poderão, sem aviso prévio, ser bloqueadas ou limitadas para todos os grupos em benefício do uso institucional.

Art. 18. Os grupos de acesso serão definidos por áreas, de modo que os acessos sejam compatíveis com a natureza das atribuições de cada setor ou grupo de usuários a saber: Visitantes, conselheiros, gabinete, presidência, assessoria técnica, jurídico, financeiro, administrativo, comunicação, tecnologia, ouvidoria/auditoria/controladoria, gerência executiva, gestão de pessoas e finalístico.

Art. 19. Os bloqueios referentes a cada grupo estão no Anexo Único desta Política.

§1° Os bloqueios ou permissões relacionados no Anexo Único poderão sofrer alterações, submetidas para aprovação do CGD.

§2° A versão atualizada será publicada na intranet e conforme a necessidade em local de acesso público no site do CFQ.

Art. 20. O bloqueio de sítios e serviços são realizados automaticamente por inteligência artificial pelos sistemas de segurança de internet da administração central do CFQ.

§1° Os sítios e serviços bloqueados equivocadamente e necessários ao desempenho das atribuições funcionais do usuário serão liberados mediante solicitação devidamente justificada e autorizada pelo gerente da unidade, via abertura de chamado na Central de Serviços.

§2° Para liberação de acesso às redes sociais e demais sítios eletrônicos, será necessária a requisição fundamentada via chamado técnico, aberto pelo dirigente da unidade - Chefe , Coordenador, Gerente, Gerente-Executivo, Ouvidor, via abertura de chamado na Central de Serviços.

Art. 21. Os casos que necessitem de tratamentos específicos devem ser encaminhados a GETIC pelo gerente ou autoridade equivalente em sua área, via abertura de chamado na Central de Serviços.

Art. 22. As solicitações de liberação a sítios eletrônicos bloqueados serão submetidas à GETIC que fará a análise técnica em relação à verificação do conteúdo e vulnerabilidades de segurança, emitindo seu parecer para deliberação no âmbito do Comitê de Governança Digital.

CAPÍTULO II

DO MONITORAMENTO

Art. 23. O acesso à internet pelos usuários da rede do CFQ deverá ser monitorado pela GETIC para fins de verificação e controle do volume de dados trafegados.

Art. 24. A GETIC produzirá, semestralmente, relatórios gerenciais com informações que possibilitem a tomada de decisão sobre o volume e a demanda de uso da Internet no CFQ.

Art. 25. As informações monitoradas incluem os endereços acessados e seus respectivos horários de acesso, sendo processadas com parâmetros gerais, sem personalização.

Art. 26. Para fins de auditoria, avaliação de controle interno, gestão de riscos e processos administrativos, o Presidente, Gerente-Executivo, Chefe de Gabinete, Gerente, Ouvidor, poderão solicitar de forma fundamentada, via processo, relatório com as informações de acesso da internet de quaisquer usuários, limitada as informações aos sites acessados e seu respectivo horário de acesso.

Art. 27. Para fins de sindicância investigativas, processos administrativos disciplinares ou éticos, o Coordenador e Membros de Comissões de Sindicância e Comitê de Ética poderão solicitar, de forma fundamentada, via processo, relatório com informações de acesso a internet relativa aos usuários interessados para fins de confirmação de suspeita de descumprimento das regras previstas na POSIN em vigor e demais normas complementares.

CAPÍTULO III

DISPOSIÇÕES FINAIS

Art. 28. É de responsabilidade da GETIC garantir os serviços de transferência e compartilhamento de arquivos com informações do CFQ na internet de forma segura.

Art. 29. A GETIC deverá homologar softwares ou serviços de mensagens instantâneas, de voz, de videoconferência e de transferência de arquivos via internet.

Art. 30. Os usuários da rede deverão comunicar à ETIR acerca dos incidentes que afetam a segurança dos ativos ou o descumprimento das regras previstas na POSIN.

Art. 31. Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a área de gestão de incidentes deverá ser imediatamente acionada, via Central de Serviços.

Art. 32. Os usuários da rede que descumprirem as regras estabelecidas por esta Portaria poderão ter, mediante decisão fundamentada seu acesso à rede bloqueado até a apuração de responsabilidades.

Art. 33. A GETIC terá o prazo de até 12 meses para implementar os controles necessários para a gestão da segurança cibernética relacionada ao conteúdo da Política.

Art. 34. Os casos omissos serão resolvidos pelo Comitê de Governança Digital.

Art. 35. Esta Portaria entra em vigor nesta data.

Dê-se ciência.

Publique-se.

Brasília, 9 de agosto de 2024.

JOSÉ DE RIBAMAR OLIVEIRA FILHO

Presidente

SCS Quadra 09, Edifício Parque Cidade Corporate, Torre B, 9º andar
Brasília/DF, CEP 70.308-200
Telefone: (61) 2099-3300 - www.cfq.org.br

ANEXO ÚNICO

GRUPOS E BLOQUEIOS

ESTRATÉGIAS/ POLÍTICAS	VISITANTES	CONSELHEIROS	GAB/PRES/ ASTEC	JURÍDICO	FINANCEIRO	ADM	COMUNICAÇÃO	TECNOLOGIA	OUVIDORIA/ AUDITORIA/ CONTROLADORIA	GEREX	GEPES	GEOF
ANÚNCIOS	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar
CONSELHOS	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
ÁLCOOL	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
ASTROLOGIA	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
BLOGS	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar
EMPRESAS	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
COMPUTADORES E SOFTWARE	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
EDUCAÇÃO	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
ENTRETENIMENTO	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar
COMPARTILHAMENTO DE ARQUIVOS	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
FINANÇAS	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
COMIDA	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
JOGOS DE AZAR	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
JOGOS	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
GOVERNO	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir

HACKING	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
ÓDIO	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
SAÚDE	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
HOBBIES	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
HOSPEDAGEM	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
MENSAGENS INSTÂNTANEAS	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
BUSCA DE TRABALHO	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
CRIANÇAS	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar
ESTILO DE VIDA	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar
CONTEÚDO ADULTO	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
NARCÓTICOS	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
NOTÍCIAS	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
NAMORO ONLINE	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
PAGAMENTO ONLINE	Bloquear	Bloquear	Bloquear	Bloquear	Permitir	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
FOTOS ONLINE	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar
FARMÁCIA	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
PORNOGRAFIA	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
PORTAIS	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
RÁDIOS ONLINE	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
IMOBILIÁRIA	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear

RELIGIÃO	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
FRAUDE	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
MECANISMOS DE BUSCA	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
REDES SOCIAIS	Bloquear	Bloquear	Permitir	Bloquear	Bloquear	Bloquear	Permitir	Bloquear	Permitir	Bloquear	Permitir	Bloquear
SOCIEDADE	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
PIRATARIA	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
ESPORTES	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar
SUICÍDIO	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
TABLÓIDES	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar
LADRÕES DE TEMPO	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
TABACO	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
VIAGEM	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar
VÍDEOS	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar	Alertar
ARMAS	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
WEBMAIL	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir	Permitir
WEB PROXY	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear
SITIOS PREPARATÓRIOS PARA CONCURSO	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear	Bloquear