REGULAMENTO INTERNO DE SEGURANÇA DA INFORMAÇÃO

R.I.S.I.

VERSÃO 1.3

DOCUMENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E INFRAESTRUTURA

INSTITUTO DE ESTUDOS DE PROTESTO DE TÍTULOS DO BRASIL (IEPTB)
COM APOIO E SUPERVISÃO DA CONSULTORIA MULTIP

ABRIL/2024

RISI IEPTB
Regulamento Interno de Segurança da Informação do Instituto de Estudos de Protesto de Títulos do Brasil

Ficha técnica deste documento

Documento	RISI IEPTB
Versão	1.3
Data da Versão	18/03/2024
Criado Por:	Márcio Bordignon (Multip)
Revisado Por:	Rodrigo Fontoura L. M. Esteves
Aprovado Por:	Comitê Gestor de SI do IEPTB
Vigência:	A partir de 08/04/2024
Nível de Confidencialidade	Público, uso interno no IEPTB
Número de Páginas	Este documento contém 12 páginas

Histórico de Alterações e Aprovações

Data	Versão	Editado por	Descrição da Alteração / Aprovação
30/09/20	Draft 1.0	Márcio Bordignon	Esboço do documento
24/11/20	Versão 1.1	Rodrigo Fontoura	Emissão da versão 1.1
11/02/21	Versão 1.2	Márcio Bordignon	Emissão da versão 1.2
18/03/24	Versão 1.3	Márcio Bordignon	Emissão da versão 1.3. Proibição de uso de credenciais corporativas para fins particulares (item 3.4.5.4)
24/04/24	Versão 1.3	Rodrigo Fontoura	Adequação de layout e ajuste da vigência (item 8.2)

Controle de impressão

A versão digital deste documento é a versão mais recente. É responsabilidade de cada indivíduo garantir que qualquer versão impressa seja a versão mais recente. A versão impressa deste documento não é controlada e não pode ser invocada, exceto quando formalmente emitido e assinado pelo Controlador de Documentos e fornecido com indicação de controle de cópia, conforme indicado nos campos abaixo:

Versão:	*1.3*
Data da Emissão:	*24/04/2024*
Cópia Controlada	**X**
Cópia não Controlada	

Sumário

Ficha técnica deste documento 1
Controle de impressão 1
Resumo Executivo 2
1. Definições e Conceitos 3
2. Sobre Responsabilidades e Proibições 4
3. Sobre Controles de Acesso 6
4. Sobre Direitos e Expectativas 8
5. Sobre Trabalho e/ou Acesso Remoto 10
6. Sobre regras de conduta em Redes Sociais 10
7. Sobre as Penalidades em caso de descumprimento 11
8. Sobre as Penalidades em caso de descumprimento 11

Resumo Executivo

Este regulamento tem por finalidade estabelecer as regras e condutas de uso aceitável para orientar os usuários do IEPTB a criar e manter a cultura de proteção à informação, em alinhamento com a Política de Segurança da Informação do IEPTB, orientando os colaboradores e Agentes quanto ao uso correto e aceitável dos recursos de Tecnologia da Informação e Comunicação (TIC), definindo responsabilidades para os usuários de TI do IEPTB, estabelecendo os privilégios e restrições de uso dos recursos de TI, protegendo os dados e informações independentemente de onde e da forma em que se encontrem disponíveis, os procedimentos a serem adotados, os direitos e expectativas de privacidade, e definindo as penalidades aplicáveis em caso de descumprimento.

1. Definições e Conceitos

- **Autenticidade:** atributo que estabelece a fidedignidade e/ou legitimidade de dado, informação, usuário, identidade da pessoa que solicita acesso à um ativo, aplicada na origem e/ou no destino.
- **Confidencialidade:** propriedade da informação para que a mesma não seja disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização. Característica da informação que está disponível somente para acesso exclusivo de pessoas ou sistemas autorizados. Atributo que define o grau de sigilo, permitindo identificar os privilégios necessários para acesso e restrições de uso.
- **Disponibilidade:** propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada. Característica de informações e/ou sistemas de ser acessado(a) por pessoas e/ou sistemas autorizadas quando for necessário. Atributo que define a capacidade de um usuário ou sistema em obter acesso à informação armazenada mediante os meios de acesso legítimos disponíveis.
- **Integridade:** propriedade ou atributo que define a exatidão da informação e sua capacidade de se manter exata mediante tentativa de modificação legítima ou ilegítima.
- **Componentes de Tecnologia da Informação e Comunicação:** São os equipamentos (tais como microcomputadores, impressoras, periféricos), softwares (tais como programas, manuais), mídias (tais como CDs, disquetes), links de acesso (tais como Internet, linhas de telefone), dispositivos e/ou componentes, bens e direitos e demais recursos tecnológicos utilizados na obtenção, produção, tratamento, processamento, armazenamento, transmissão e recuperação da informação, incluindo a própria informação.
- **Dados e Informações:** São todos os documentos, informações ou dados recebidos, armazenados, gerados ou processados pelo IEPTB, independente de seu meio de armazenamento (tais como servidores, computadores, mídias de computador ou papel impresso).
- **Dados Pessoais:** Dados que permitem identificar uma pessoa natural, conforme definição da Lei 13.709/2018 (LGPD).
- **Dados Pessoais Sensíveis:** Dados que permitem discriminar uma pessoa natural, conforme definição da Lei 13.709/2018 (LGPD).
- **Usuário:** é toda pessoa que possui acesso à dados, informações ou ativos de TIC do IEPTB.
- **Suporte Técnico:** equipe formada por colaboradores do setor de TI do IEPTB e/ou de empresa terceirizada responsável pelos assuntos relacionados à Tecnologia de Informação.
- **Incidente de Segurança:** evento ou série de eventos adversos, indesejados ou inesperados, confirmado ou sob suspeita, relacionado ao comprometimento da integridade, disponibilidade ou autenticidade de ativos ou ao bom funcionamento do negócio da organização, tais como (mas não limitado a) ataques, uso ou acesso não autorizado, vírus, vazamento de informação ou mesmo violação à Política de Segurança.
- **Autenticação:** processo utilizado para estabelecer a autenticidade e/ou legitimidade da pessoa ou sistema que solicita ou faz uso de dados ou Componentes de Tecnologia da Informação e Comunicação.
- **Credenciais de Acesso:** conjunto de informações de usuário dos recursos de TIC, composto por Login, Senha ou outros fatores, que possibilitem acesso a estes recursos.
- **Login:** palavra utilizada para identificar o usuário durante o processo de autenticação.
- **Senha:** palavra secreta, de conhecimento exclusivo do usuário, que permite validar o login do mesmo durante o processo de autenticação.
- **Log:** arquivo contendo o registro das operações de usuários realizadas por meio do uso dos ativos de TIC, armazenado com o objetivo de identificar qual a operação realizada, como, quando, onde e por quem foi realizada.
- **Operação:** toda e qualquer atividade de manuseio, tratamento ou manipulação de informação.
- **Ameaça:** fato, ação, gesto ou palavra que intimida, atemoriza ou se constitui em sinal ou indício de acontecimento desfavorável ou maléfico. Violência moral, destinada a perturbar a liberdade psíquica e a tranquilidade da vítima, pela intimidação ou promessa de causar a alguém, futura ou imediatamente, mal relevante e injusto.
- **Calúnia:** imputar falsamente a alguém fato definido como crime.
- **Difamação:** desacreditar publicamente uma pessoa, maculando-lhe a reputação.
- **Injúria:** Ofensa à dignidade ou decoro de alguém.
- **Hacker:** Denominação genérica para pessoa com grande habilidade em computação.
- **Cracker:** pessoa que utiliza sua grande habilidade em computação para fins maléficos.
- **Carders:** infratores especializados na fraude, falsificação e clonagem de cartões (de crédito, magnéticos, telefônicos, etc) para utilização fraudulenta.

- **Phreackers:** pessoas que burlam sistemas de telecomunicações.
- **Malware ou Vírus:** programa de computador malicioso, cujo funcionamento provoca dano, perda de informação, quebra do sigilo, lentidão, quebra de sigilo, quebra de integridade ou perda da confiabilidade ou comportamento indesejado de Componentes de Tecnologia da Informação.
- **Rastreamento:** registro da origem, do destino, da data e hora, da natureza da comunicação e dos usuários envolvidos em arquivos armazenados ou transferência de dados ocorrida entre computadores, sem que o conteúdo das mensagens seja inspecionado ou revelado.
- **Monitoramento:** verificação do conteúdo das mensagens, arquivos e dados armazenados, transmitidos, enviados ou recebidos por computadores do Instituto de Estudos de Protesto de Títulos do Brasil (IEPTB).
- **Não-repúdio ou irretratabilidade:** Capacidade de prevenir a rejeição ou repúdio por parte do autor ou do receptor de uma operação, mensagem, informação ou dado, impedindo a ocorrência de negação ilegítima, falso positivo ou falso negativo.

2. Sobre Responsabilidades e Proibições

2.1. Cabe à Gerencia de TI do IEPTB a responsabilidade de acompanhar a aplicação da política de segurança da informação, no uso de suas atribuições.

2.2. **É DEVER DE TODOS** considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para o IEPTB e deve sempre ser tratada profissionalmente.

2.3. Cabe à Gerencia de TI do IEPTB a responsabilidade de elaborar, implementar, manter em funcionamento, cumprir e fazer cumprir as rotinas, procedimentos, planos e projetos de informatização do IEPTB

2.3.1. Cabe ao Comitê Gestor de Segurança da Informação (CGSI) do IEPTB, em conjunto com a Gerencia de TI, definir, implementar e monitorar os aspectos de segurança da informação relacionados a estas atividades.

2.3.2. O Regulamento Interno de Segurança da Informação pode ser atualizado conforme as necessidades do IEPTB, a qualquer tempo, e as atualizações passam a vigorar a partir da data de sua aprovação pela Direção Geral.

2.4. Cabem aos usuários zelar pela integridade, confidencialidade e disponibilidade dos ativos de tecnologia da informação e comunicação (equipamentos, dados, informações, softwares, links) que lhe são confiados pelo IEPTB, fazendo uso destes recursos estritamente para cumprir com suas atividades profissionais e de acordo com as práticas recomendadas, na forma descrita neste regulamento e das normas vigentes no IEPTB.

2.4.1. Os usuários deverão zelar pelo correto uso dos Componentes de Tecnologia da Informação e dispositivos de processamento e tratamento de dados disponibilizados para seu uso profissional, com especial atenção para detecção e notificação de incidentes de segurança, informando imediatamente à equipe de Suporte Técnico qualquer anormalidade observada

2.4.2. É vedado ao usuário utilizar os ativos e componentes de tecnologia da informação e comunicação (tais como endereço de e-mail, equipamentos, softwares, impressoras, suprimentos, informações, dados, acesso à Internet, links e demais recursos de processamento de dados e informações) para uso pessoal (diverso do uso profissional) ou com a finalidade de:

- Prestar serviços à outras pessoas (físicas ou jurídicas) que não o IEPTB, com ou sem a finalidade de obter lucro ou vantagem;
- Divulgar, promover ou participar de campanhas, promoções, correntes, pirâmides;
- Enviar, divulgar, promover, prover o acesso (ou meios de acesso) ou participar de campanhas, grupos de discussão ou mensagens cujo conteúdo seja preconceituoso, difamatório, calunioso, injurioso, ameaçador ou ilegal;
- Divulgar, promover, participar, prover o acesso ou os meios de acesso à pessoas, grupos de discussão, sites e comunidades cujo conteúdo seja preconceituoso, violento, ofensivo, discriminatório, erótico, pornográfico, terrorista, criminoso ou relacionado à fanatismo de

qualquer espécie, que defendam atividades ilegais, Que menosprezem, depreciem ou incitem o preconceito a determinadas classes, que violem os direitos aos titulares de dados pessoais, que permitam a transferência (downloads) de arquivos e/ou programas ilegais, entre outros conteúdos prejudiciais ao IEPTB;

- Acessar, instalar, armazenar, copiar, reproduzir ou violar os direitos de software ou conteúdo protegido por direitos autorais (pirataria), no todo ou em parte, para uso próprio ou para terceiros, sem possuir a respectiva licença de uso, ou utilizando o software, programa ou arquivo de forma diversa daquela estipulada em seu contrato de licenciamento;
- Acessar, instalar, armazenar, copiar, reproduzir ou utilizar programas de computador com código malicioso (vírus, spyware, troianos) ou ferramenttas hacker, cracker, carder ou phreacker;
- Divulgar a alguém, sem justa causa, conteúdo de documentos, dados, informações ou correspondências classificadas pelo IEPTB como restritas, sigilosas ou confidenciais, de que é destinatário ou detentor;
- Divulgar a alguém, sem justa causa, segredo de que tem ciência em razão da função, ofício ou profissão;
- Violar os termos de serviço dos provedores e sistemas de informação acessados;
- Obter ou tentar obter acesso não-autorizado à outro dispositivo, computador, servidor, sistema ou rede, componente de tecnologia de Informação, dados, informações ou ativos;
- Interromper ou degradar desempenho de serviço, dispositivos, componentes, servidores ou rede de computadores por sobrecarga ou por meios ilegítimos, ilícitos ou maliciosos;
- Burlar ou tentar burlar qualquer sistema de segurança e/ou proteção;
- Vigiar secretamente ou assediar terceiros;
- Acessar informações confidenciais de qualquer natureza para as quais não esteja credenciado;
- Acessar informações confidenciais, de qualquer natureza (tais como nome de Login e senha de acesso de outro usuário que esteja vulnerável);
- Utilizar dos recursos de TI e da conexão à Redes e/ou Internet do IEPTB para fins de lazer, diversão e entretenimento.

2.4.3. Em caso de furto, roubo, perda ou extravioo de dispositivo móvel de propriedade e/ou contendo dados do IEPTB, o usuário deverá providenciar as seguintes medidas:

2.4.3.1. Comunicar imediatamente o Suporte Técnico e o seu superior imediato.

2.4.3.2. Registrar ocorrência em uma delegacia de polícia, e disponibilizar cópia do Boletim de Ocorrência para o Suporte Técnico.

2.4.4. O Suporte Técnico está orientado a verificar e eliminar periodicamente a eliminar todas as informações e dados de violarem este regulamento, bem como todos os compartilhamentos existentes nas estações de trabalho, e garantir que dados considerados confidenciais e/ou restritos não estejam armazenados indevidamente.

2.4.5. O usuário que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ilícito (Art. 186 do Código Civil).

2.4.5.1. Aquele usuário que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo.

2.4.5.2. O usuário estará obrigado de reparar o dano, independentemente de culpa, nos casos específicados em Lei, ou quando a atividade desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem

2.4.5.3. Nos casos em que o usuário observar, perceber ou suspeitar da ocorrência de incidente de segurança ou do uso não autorizado dos recursos de TIC, deverá comunicar o Suporte Técnico imediatamente

2.4.5.3.1. Quando da ocorrência de incidente de segurança, sinistro, ataque bem sucedido ou violação de uso dos recursos e ativos de TIC, o usuário deverá preservar a maior quantidade possível de evidências relevantes, para permitir a realização de perícia

2.4.6. Os Diretores, Gerentes e supervisores do IEPTB são responsáveis por:

2.4.6.1. Definições dos direitos de acesso de seus funcionários subordinados, aos sistemas e informações do IEPTB, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

2.4.6.2. Advertir e aplicar penalidades aos seus subordinados que cometerem as infrações previstas neste regulamento no exercício de suas funções, de forma a evitar indulgência ou condescendência que possa prejudicar o IEPTB

2.4.6.3. Respeitar este regulamento, como qualquer usuário

2.4.7. O Gerencia de TI fará auditorias periódicas do acesso dos usuários às informações, verificando:

2.4.7.1. Que tipo de informação o usuário pode acessar;

2.4.7.2. Quem está autorizado a acessar determinada rotina e/ou informação;

2.4.7.3. Quem acessou determinada rotina e informação;

2.4.7.4. Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;

2.4.7.5. Que informação ou rotina determinado usuário acessou;

2.4.7.6. Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

2.5. Dados Pessoais e Dados Pessoais de Colaboradores não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se mas não limitando-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários do IEPTB. Por outro lado, os colaboradores se comprometem a não armazenar dados pessoais nas instalações do IEPTB, sem prévia e expressa autorização por parte da diretoria.

2.5.1. Mesmo que seja autorizado o armazenamento destes dados, O IEPTB não se responsabiliza por eles, nem tampouco pelo seu conteúdo e respectiva segurança. Tais dados jamais poderão ser armazenados nos Componentes de Tecnologia da Informação e Comunicação do IEPTB, e jamais poderão fazer parte da(s) rotina(s) de backup.

3. Sobre Controles de Acesso

3.1. A Direção Geral do IEPTB, por meio do Comitê Gestor de Segurança da Informação (CGSI) , define as medidas aplicáveis para proteger fisicamente e logicamente os ativos e componentes de Tecnologia da Informação.

3.2. Os usuários obterão acesso aos recursos de informática de uso comum, acesso à Internet, e-mail, sistemas de informação e áreas de armazenamento em servidores mediante autenticação de sua credencial de acesso, e deverão utilizar estes recursos como meio de armazenamento de seus arquivos de trabalho

3.2.1. Os dispositivos de armazenamento (mídias locais) instalados nos computadores utilizados como estação de trabalho dos usuários não possuem proteções de cópia de informações (backup).

3.2.1.1. Não é política do IEPTB o armazenamento de dados em desktops individuais, entretanto, existem alguns programas que não permitem o armazenamento em rede. Nestes e em outros casos, o Suporte Técnico deverá providenciar solução de backup ou alertar ao usuário que ele deve fazer backup dos dados de sua máquina periodicamente.

3.2.1.2. É responsabilidade dos próprios usuários a elaboração de cópias de segurança (“backups”) de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios do IEPTB.

3.2.1.3. Caso os usuários optem por armazenar informações ou arquivos nas mídias locais dos computadores que utilizam serão responsáveis pela integridade, confidencialidade e disponibilidade destas informações.

3.2.1.4. No caso das informações consideradas de fundamental importância para a continuidade dos negócios do IEPTB, o Suporte Técnico disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas nas rotinas de backup.

3.3. Toda mídia proveniente de entidade externa ao IEPTB deve ser verificada contra malware, assim como todo arquivo recebido e/ou obtido através do ambiente Internet. Todos os dispositivos e estações de trabalho devem ter um software de proteção (endpoint) contra malware e ameaças comportamentais instalado. A atualização do endpoint será automática, agendada pelo setor de Informática, via rede. O usuário não pode em hipótese alguma, desabilitar a proteção endpoint instalada nos dispositivos que usa.

3.4. Para uso dos recursos e dispositivos de informática do IEPTB, o usuário receberá credenciais de acesso à estes dispositivos, à rede do IEPTB e aos sistemas necessários às suas atividades laborais, composta – no mínimo - de um nome de "Login" e uma senha.

3.4.1. As credenciais de acesso são pessoais e intransferíveis. Em hipótese alguma o usuário poderá revelar, divulgar ou ceder sua credencial para outrem, independente de posição hierárquica, exceto quando requisitado por autoridade do poder policial ou judiciário legalmente constituída para requerer esta cessão.

3.4.2. É dever do usuário zelar pelo sigilo de sua credencial de acesso, mantendo as informações de Login e sua respectiva senha protegidas contra acesso de terceiros.

3.4.3. É dever do usuário zelar pelo sigilo de documentos e informações digitais e também impressos e/ou em mídia física, mantendo seu ambiente de trabalho organizado e protegido contra acesso de terceiros, conforme procedimentos de Mesa Limpa e de Tela Limpa vigentes no IEPTB.

3.4.4. Em caso de extravio, perda ou roubo das informações de credencial de acesso ou de componente/dispositivo, o usuário deverá comunicar ao Suporte Técnico imediatamente, para que este cancele os privilégios de acesso da credencial extraviada e conceda nova credencial de acesso à este usuário.

3.4.5. A solicitação para criação, modificação ou exclusão de conta de acesso de usuário é de responsabilidade das Gerências das Equipes, que deverão encaminhar formalmente solicitação à Secretaria de RH para providências, informando - no caso de inclusão ou modificação - quais rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

3.4.5.1. A formalização da solicitação e de seu respectivo atendimento deverá observar os critérios e determinações dos procedimentos para tal fim vigentes no IEPTB.

3.4.5.2. A credencial inicialmente concedida ao usuário é composta de uma senha padrão, fornecida imediatamente pela equipe de Suporte Técnico ao usuário no ato de sua criação. Ao receber sua credencial de acesso, o usuário será solicitado pelo sistema de autenticação do IEPTB a mudar sua senha, tornando-a secreta.

3.4.5.3. Por segurança, a área de TI recomenda que as senhas tenham sempre um critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

3.4.5.4. O usuário é proibido de utilizar a credencial de acesso (login e senha) de uso corporativo aos sistemas e dados do IEPTB para fins pessoais.

3.4.6. As Gerências das Áreas são responsáveis por comunicar à Secretaria de RH os(as) substitutos(as) de colaboradores quando de sua ausência do IEPTB, bem como comunicar também o retorno dos(as) colaboradores ausentes, para que as permissões de acesso aos sistemas e ativos de informação possam ser adequadas, documentadas e rastreadas.

3.5. A instalação, desinstalação, configuração e manutenção de componentes (software, hardware, rede, etc) é prerrogativa **exclusiva e restrita** à equipe de Suporte Técnico.

3.5.1. O Suporte Técnico é responsável pela aplicação da Política de Segurança da Informação do IEPTB em relação a definição de compra e substituição de "software", "hardware" e componentes. Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática. Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

3.5.2. O IEPTB respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, proibindo o uso de programas não licenciados nos computadores da organização. É terminantemente proibido o uso de programas ilegais (Sem licenciamento) no IEPTB.

3.5.2.1. Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos IEPTB, mesmo porque somente o pessoal da área de TI tem autorização para instalação de programas previamente autorizados dentro da política de segurança da companhia. Periodicamente, o Setor de Informática verificará os dados dos servidores e/ou os computadores/dispositivos dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes serão removidos dos computadores.

3.5.2.2. Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados, se responsabilizam perante o IEPTB por quaisquer problemas ou prejuízos causados oriundos desta ação, estando sujeitos as sansões previstas neste documento.

3.5.3. Os compartilhamentos de impressoras devem estar sujeitos à autorizações. Não são permitidos no IEPTB o compartilhamento de dispositivos móveis tais como pen-drivers e outros.

3.5.4. O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais no IEPTB. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados. O uso da Internet será rastreado pelo Suporte Técnico, inclusive através de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

3.5.4.1. A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição das chefias imediatas dos usuários, com base em recomendação do Suporte Técnico. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso conforme descrito no item 2.4.2 deste regulamento.

4. Sobre Direitos e Expectativas

4.1. O acesso à Internet, ao e-mail e aos demais recursos de informática do IEPTB são passíveis de rastreamento e monitoramento.

4.1.1. O e-mail corporativo (com o domínio @cartoriosdeprotesto.org.br) e os componentes e dispositivos de propriedade do IEPTB e fornecidos para uso de seus colaboradores são ferramentas/instrumentos de trabalho proporcionadas pelo empregador/contratante ao empregado/contratado ou colaborador, com a finalidade da consecução do serviço profissional para a realizaçào do negócio do IEPTB, e são passíveis de rastreamento e monitoramento

4.1.1.1. O correio eletrônico fornecido pelo IEPTB é um instrumento de comunicação interna e externa para a realização do negócio do IEPTB. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do IEPTB, não podem ser contrárias à legislação vigente e nem aos princípios éticos do IEPTB.

4.1.1.2. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do IEPTB, não podem ser contrárias à legislação vigente e nem aos princípios éticos do IEPTB.

4.1.1.3. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens em desacordo com as orientações deste regulamento, em especial aquelas definidas no item 2.4.2.

4.1.1.4. Não será permitido o uso de e-mail gratuitos (liberados em alguns sites da web), nos computadores do IEPTB. O Suporte Técnico poderá, visando evitar riscos cibertnéticos ou de vazamento de dados, bloquear o recebimento de e-mails provenientes de sites não autorizados previamente.

4.1.2. O simples acesso aos recursos de informática e comunicações colocados à disposição do empregado pelo empregador (tais como e não limitados a e-mail ou mensagens SMS) não implica em requisição de trabalho.

4.1.3. O recebimento de mensagens pelo usuário na sua caixa postal corporativa ou em outros dispositivos pode ocorrer em horário diverso ao desenvolvimento das atividades funcionais. O fato de ter acesso ao recurso, por si só, não representa solicitação a trabalhar.

4.1.4. A equipe de Suporte Técnico fica autorizada a rastrear, se necessário for, os acessos dos usuários à rede Internet, intranet e extranet, seja por meios diretos ou aplicativos (ferramentas) específicos, em tempo real ou posteriormente ao uso, identificando a origem e o destino das mensagens e comunicações.

4.1.5. Os arquivos, documentos e informações armazenados nos computadores, servidores e estações de trabalho do IEPTB são passíveis de monitoramento pelo Suporte Técnico. A equipe de Suporte Técnico somente estará autorizada a monitorar o conteúdo dos arquivos, mensagens e comunicações realizadas por usuários quando solicitada – de maneira oficial - pela Diretoria Geral do IEPTB.

4.2. Ao usuário é permitido e em alguns casos será exigido o uso, desde que previamente autorizado e/ou comunicado pelo Comitê Gestor de Segurança da Informação do IEPTB, de programas de criptografia com o objetivo de proteger o sigilo de arquivos, documentos e mensagens.

4.2.1. Os programas de criptografia utilizados devem estar de acordo com a legislação vigente no Brasil

4.2.2. O usuário que optar por utilizar programas de criptografia é responsável por zelar pela integridade e disponibilidade da chave de acesso.

4.3. A proteção do recurso computacional (componentes) de uso individual é de responsabilidade do próprio usuário. É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.

4.3.1. O usuário não deve alterar a configuração do equipamento recebido.

4.3.2. Alguns cuidados que devem ser observados:

4.3.2.1. Fora do local de trabalho (sede do IEPTB):

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

4.3.2.2. Em caso de furto

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao Setor de Informática;
- Envie uma cópia da ocorrência para o Setor de Informática.

4.4. Os usuários que tiverem direito ao uso de dispositivos pessoais (celulares, tablets, laptops ou notebooks), ou qualquer outro equipamento computacional, devem estar cientes de que:

4.4.1. É proibido o uso destes dispositivos para acessar, tratar ou armazenar dados e informações do IEPTB

4.5. O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos do IEPTB, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade exclusiva do Suporte Técnico, de acordo com as definições da política de Segurança da Informação do IEPTB.

4.6. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IEPTB é considerado patrimônio do IEPTB e deve ser protegida conforme estabelecido neste RISI.

4.7. É de propriedade do IEPTB, todos os "designs", criações ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo contratual com o IEPTB.

4.8. Após a rescisão do vínculo com o IEPTB, o usuário não poderá sob qualquer pretexto, reproduzir, divulgar, revelar, ou dar conhecimento a terceiros estranhos a esta contratação, de quaisquer informações obtidas e/ou transmitidas pelo IEPTB, exceto com prévio consentimento por escrito deste, durante a vigência deste instrumento, bem como posteriormente a ele, até que as referidas informações se tornem de domínio publico.

5. Sobre Trabalho e/ou Acesso Remoto

5.1. As regras de conduta e recomendações de boas práticas para os usuários e colaboradores do IEPTB que necessitarem de realizar trabal;ho e/ou acesso remoto estão detalhadas no procedimento P00-POSI (Procedimento de Organização da Segurança da Informação do IEPTB). Todos os usuários que necessitarem de realziar trabaleho e/ou acesso remoto devem estar cientes deste procedimento, bem como formalizar sua ciência e aceitação.

6. Sobre regras de conduta em Redes Sociais

6.1. Os coalboradores e usuários do IEPTB estão proibidos de usar redes sociais para postar ou exibir comentários sobre colegas de trabalho, supervisores ou terceiros que sejam vulgares, obscenos, ameaçadores, assediadores ou que caracterizem uma violação de nossas políticas de discriminação ou assédio.

6.2. A equipe não pode usar as redes sociais para divulgar qualquer informação proprietária e/ou confidencial do IEPTB ou de seus funcionários, clientes ou parceiros de negócios.

6.3. Quando apropriado, os funcionários devem divulgar seu relacionamento com o IEPTB em suas postagens online e abster-se de falar em nome do IEPTB quando não estiver autorizado a fazê-lo.

6.4. Cada usuário e/ou colaborador do IEPTB deve ter em mente que é pessoalmente responsável pelo que publica online, e estar ciente de que o que disser/postar ficará disponível publicamente por um longo período de tempo.

6.5. O uso de mídia social está sujeito às mesmas políticas de local de trabalho que a equipe deve seguir em outras situações, incluindo, mas não se limitando às nossas políticas relativas a assédio, discriminação, difamação, confidencialidade, não concorrência e uso geral da Internet.

7. Sobre as Penalidades em caso de descumprimento

7.1. O usuário que infringir o presente regulamento ficará sujeito à penalidades previstas nas normas, regulamentos e Contratos do IEPTB que tratam das relações entre o Escritório e seus colaboradores.

7.1.1. O não cumprimento deste Regulamento implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

8. Sobre a vigência e abrangência deste Regulamento

8.1. Este regulamento passa a vigorar na data de sua aprovação pela Direção Geral do IEPTB, e a produzir seus efeitos sobre cada usuário após a assinatura de cada um no seu respectivo Termo de Ciência.

8.2. Este regulamento pode ser alterado ou modificado a qualquer tempo, e suas modificações passam a vigorar mediante nova aprovação pelo Conselho Gestor de Segurança da Informação e sua publicação. Um comunicado informativo interno deve ser disparado para informar os colaboradores acerca das alterações e/ou atualizações.

São Paulo, 24 de abril de 2024

gov.br
Documento assinado digitalmente
RODRIGO FONTOURA LOPES MARTINS ESTEVES
Data: 16/05/2024 17:45:31-0300
Verifique em https://validar.iti.gov.br