



POLÍTICAS DE SEGURANÇA DA
INFORMAÇÃO

FADISP
FACULDADE AUTÔNOMA DE DIREITO

FACULDADE AUTÔNOMA DE DIREITO

Recredenciamento pela Portaria MEC Nº. 1.211, de 26 de outubro de 2016
Publicada no Diário Oficial da União Nº 208, Seção I, de 28/10/2016, pág. 24

RESOLUÇÃO nº 015/2023, de 16 de janeiro de 2023.

*Aprova as Políticas de Segurança da
Informação,*

O Diretor Superintendente da Faculdade Autônoma de
Direito – FADISP, no uso de suas atribuições regimentais,

RESOLVE:

Art. 1º Aprovar as Políticas de Segurança da Informação da Faculdade
Autônoma de Direito – FADISP.

Art. 2º Esta Resolução entra em vigor na data de sua assinatura.

São Paulo, 16 de janeiro de 2023.


Dr. Nelson de Carvalho Filho
Diretor Superintendente da Faculdade Autônoma de Direito

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

OBJETIVO

Estabelecer os princípios de Segurança da Informação da Faculdade Autônoma de Direito – FADISP, regulamentar a forma de uso dos recursos fornecidos e definir as sanções aplicáveis nos casos de descumprimentos das regras de uso.

1. APLICAÇÃO

Esta política é aplicável a todos aqueles que utilizam os recursos da FADISP, funcionários, prestadores de serviço e visitantes.

2. RESPONSABILIDADE

2.1 *Tecnologia da Informação:*

- Definir as diretrizes estratégicas de segurança da informação para a empresa;
- Realizar auditorias nos equipamentos da rede FADISP, quando necessário;
- Manter os softwares sempre atualizados, conforme disponibilizado pelos fabricantes, seguindo as diretrizes de controle de mudanças;
- Bloquear os acessos dos usuários que possam estar realizando quaisquer atividades consideradas nocivas às informações;
- Instalar softwares que garanta um nível ideal de proteção para o equipamento;
- Desinstalar quaisquer softwares que possam expor a integridade da rede;
- Credenciar/descredenciar usuários;
- Informar aos gestores e/ou RH acerca da má utilização das ferramentas de T.I para aplicação de sanções e/ou punições cabíveis.

2.2 *Gerentes, Coordenadores e Supervisores:*

- Ministrando treinamento aos colaboradores, divulgando a Política de Segurança da Informação;
- Solicitar quaisquer necessidades de novas ferramentas/softwarees ao T.I para avaliação do impacto quanto à segurança da informação;
- Cumprir todas as normas e rotinas descritas neste documento, entendendo as consequências, sanções e/ou punições cabíveis.

2.3 *Demais colaboradores:*

- Cumprir com esta política na execução das suas rotinas, seguindo as premissas e objetivos estabelecidos;

- Comunicar aos gestores ao detectar possíveis ocorrências contrárias à Política de Segurança da Informação;
- Utilizar de forma consciente todos os recursos disponibilizados pela empresa;
- Zelar e preservar os equipamentos disponibilizados pela FADISP para execução dos trabalhos;
- Cumprir todas as normas e rotinas descritas neste documento, entendendo as consequências, sanções e/ou punições cabíveis.

3. **DEFINIÇÕES:**

- Não se aplica;

4. **REFERÊNCIAS:**

- Não se aplica;

5. **MATERIAIS/EQUIPAMENTOS:**

- Não se aplica;

6. **CONSIDERAÇÕES:**

6.1 - **Esta política aplica-se a todos os colaboradores e prestadores de serviço que possam impactar na segurança da informação da FADISP;**

6.2 - **Esta política visa proporcionar, confidencialidade, confiabilidade, integridade e disponibilidade da informação, através de mecanismos que promovam a integridade de uma estrutura de rede na qual trafegam informações e dados compartilhados/ restritos, além dos equipamentos que armazenam tais informações;**

6.3 - **A não observância desta regra sujeita o usuário a sanções descritas no item 8.16.**

7. **PROCEDIMENTO**

7.1 - **Segurança Física (Infraestrutura e Hardwares):**

7.1.1 - **A Segurança Física tem como objetivo:**

- Manter restrito o acesso a Sala dos Servidores;
- Garantir que apenas tenha acesso aos equipamentos, quem esteja devidamente qualificado para uso ou manuseio;
- Orientar e acompanhar os colaboradores que não fazem parte da equipe de TI, que venham a realizar atividades no interior da Sala dos Servidores;
- Ter procedimentos que garantam a continuidade das atividades da empresa, como plano de contingência e backup.

7.2 - **Infraestrutura Elétrica:**

7.2.1 - Todos os equipamentos e ativos de T.I são conectados em rede estabilizada ou nobreaks;

- 7.2.2 - A infraestrutura da sala de servidores é atendida por nobreaks com capacidade adequada, conforme especificação técnica do produto;
- 7.2.3 - As estações clientes, os equipamentos de distribuição da rede, bem como os equipamentos da sala de servidores estão ligados à rede de alimentação do grupo-gerador;
- 7.2.4 - Toda a infraestrutura de T.I (elétrica ou de dados) possui proteção contra descargas atmosféricas;
- 7.2.5 - Para toda estrutura elétrica existe aterramento capaz de garantir a proteção necessária em caso de descarga elétrica.

7.3 - Rede de Dados:

- 7.3.1 - A FADISP se reserva o direito de monitorar todo o tráfego da rede de computadores e utilização dos recursos de T.I a qualquer momento, para garantir a disponibilidade do serviço;
- 7.3.2 - Não será permitida a associação de qualquer tipo de equipamento à rede de computadores da empresa (rede cabeada ou rede sem fio) sem prévio conhecimento e autorização da área de T.I.;
- 7.3.3 - Acesso externo à rede de computadores da FADISP utilizando VPN será concedido somente para usuários formalmente autorizados pela área de T.I., deverá ser aberto um chamado para a área de T.I., no sistema específico para este fim.

7.4 - Segurança Ambiental:

- 7.4.1 - É de responsabilidade do Setor de Segurança do Trabalho criar e executar procedimentos que visam reduzir os riscos provenientes de força natural, como: Incêndio, Fumaça, poeira, vibração, umidade dentre outros.

7.5 - Acesso às Instalações:

- 7.5.1 - **Com o intuito de prevenir perda, dano ou comprometimento dos ativos e evitar a exposição ou roubo de informação, são adotadas as seguintes medidas:**

- As áreas com instalações de equipamentos de T.I ou de infraestrutura de T.I são restritas somente a pessoal autorizado;
- A sala de servidores, racks ou qualquer outro ativo de rede espalhados pela empresa são protegidas com portas chaveadas;
- São restritos os acessos às áreas com ativos de T.I (estações clientes e/ou equipamentos de infraestrutura), baseadas no status do funcionário e horas de operação ou atendimento de chamados;

- É proibido aos colaboradores permitir a estranhos, o acesso aos recursos de rede. Eventuais necessidades devem ser apresentadas à área de TI, para que seja avaliada a liberação.

7.6 - Equipamentos de T.I:

- 7.6.1 - O manuseio nos equipamentos de TI somente pode ser executado por pessoa devidamente qualificada, caso seja necessário a contratação de um fornecedor, o mesmo deve ser qualificado;
- 7.6.2 - Devem ser utilizados somente equipamentos homologados pela ANATEL ou órgão regulador equivalente;
- 7.6.3 - Estabelecer as condições de uso dos equipamentos fornecidos pela empresa aos colaboradores para a execução de suas funções.
- 7.6.4 - Pacotes de software de segurança disponibilizados (por ex.: antivírus, anti-spyware e firewall pessoal) deverão ser instalados em todos os equipamentos;
- 7.6.5 - Somente a área de Tecnologia da Informação, pode ter acesso a ferramentas de administração dos equipamentos, sejam eles desktops, notebooks, impressoras ou qualquer outro recurso de T.I.;
- 7.6.6 - Acesso remoto ao equipamento (computador, impressora e outros) e exclusivo a área de Tecnologia da Informação;
- 7.6.7 - O uso de dispositivos de entrada e saída será liberado somente para usuários formalmente autorizados pela área de Tecnologia da Informação, por meio solicitação da área e anuência do gestor da mesma, os quais deverão ser orientados sobre o uso adequado e responsável destes recursos;
- 7.6.8 - Ao apresentar problema o responsável pelo equipamento deverá abrir um chamado para atendimento por meio do software específico para esse fim;
- 7.6.9 - A abertura ou a remoção de qualquer equipamento de T.I só poderá ser feita pela área de Tecnologia da Informação;
- 7.6.10 - Nenhum equipamento, periférico ou componente de equipamento poderá ser retirado das dependências da FADISP sem que haja uma autorização formal da Gerência de T.I.;
- 7.6.11 - Os colaboradores que utilizarem notebooks fornecidos pela empresa deverão assinar um termo de responsabilidade sobre o equipamento. Além disso, deverão portar um Comunicado Interno (CI) de Autorização de Porte do equipamento que os permita sair da empresa portando o referido equipamento;

- 7.11.8 - A cópia de arquivos da Internet (download) será feita de forma restrita e controlada. Em se tratando de cópia software, deve ser observado o item 8.9 desta política;
 - 7.11.9 - É vedada a utilização de qualquer tipo de serviço de mensagens instantâneas não homologados pela Área de T.I., bem como programas de troca de arquivos de dados;
 - 7.11.10 - O usuário deve usar a Internet de forma adequada e diligente, observando a conformidade com as leis, a moral, a política de qualidade da empresa, os costumes socialmente aceitos e a ordem pública;
 - 7.11.11 - O acesso a sites de pornografia e outros contrários à lei é terminantemente proibido;
 - 7.11.12 - O acesso a sites de relacionamentos tais como Facebook, Twitter, Skype e outras redes sociais do mesmo gênero é terminantemente proibido;
 - 7.11.13 - O acesso a sites de instituições bancárias deve ser feito digitando o endereço diretamente no navegador Web, nunca clicando em um link existente em uma página ou em uma mensagem, ao acessar o site do banco, forneça apenas uma posição do cartão de segurança (desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição), o acesso a instituições bancárias deve ser moderado e limitado, a FADISP não se responsabiliza por fraudes que por ventura possa ocorrer com as contas pessoais;
 - 7.11.14 - Caso as atribuições profissionais do usuário o façam necessitar acessar um site bloqueado este acesso poderá ser requerido, mediante solicitação do gestor da área solicitante e autorização da Área de T.I, por meio da ferramenta de chamados da área de T.I.
- 7.12 - **Correio Eletrônico (e-mail):**
- 7.12.1 - A FADISP se reserva o direito de monitorar o conteúdo das mensagens de e-mail, quando se fizer necessário, para garantir a disponibilidade do serviço e a integridade de sua imagem;
 - 7.12.2 - A caixa de correio eletrônico (e-mail) terá, via de regra, seu tamanho limitado para todos os usuários;
 - 7.12.3 - O usuário será alertado pelo serviço de correio eletrônico toda vez que sua caixa atingir um tamanho próximo do limite. Quando o limite for ultrapassado, a caixa de e-mail do usuário será fechada para o envio e/ou recebimento de novas mensagens e só será reaberta após a eliminação do excesso de tamanho;

- 7.12.4 - O tamanho máximo das mensagens enviadas e/ou recebidas é de 25Mb independente do perfil do usuário;
 - 7.12.5 - O correio eletrônico deve ser utilizado única e exclusivamente para fins de trabalho;
 - 7.12.6 - É expressamente proibido o uso do e-mail para envio de informações classificadas como confidenciais para terceiros que não possuam vínculo com o negócio da empresa;
 - 7.12.7 - É vedado o uso do recurso de correio eletrônico para difamação, humilhação e brincadeiras de qualquer natureza;
 - 7.12.8 - É vedado o encaminhamento de mensagens de e-mail cujo conteúdo seja considerado corrente;
 - 7.12.9 - É obrigatória a utilização de assinatura nos e-mails, seguindo o formato definido pela área de T.I.;
 - 7.12.10 - Todas as mensagens excluídas enviadas para a lixeira do e-mail serão excluídas em 30 (trinta) dias, ou seja, todas as mensagens com mais de 30 dias de existência na caixa de excluídos serão automaticamente excluídas de forma definitiva.
- 7.13 - Servidor de Arquivos**
- 7.13.1 - O servidor de arquivos é liberado para armazenamento de dados de interesse da FADISP, sendo expressamente proibido o arquivamento de dados e informações que desrespeitem as leis de proteção intelectual (tais como cópias não autorizadas de softwares, músicas, vídeos e fotografias);
 - 7.13.2 - É expressamente proibido o uso do servidor de arquivos para fins pessoais, como armazenamento de música, vídeos, etc.;
 - 7.13.3 - A FADISP se reserva o direito de monitorar o conteúdo de todos os locais de armazenamento, periodicamente ou quando considerar necessário, para garantir a disponibilidade do serviço;
 - 7.13.4 - Todo conteúdo que infringir as regras desta política será automaticamente apagado sem aviso prévio. O responsável pelo armazenamento indevido do conteúdo será advertido, conforme sanções e/ou punições desta política;
 - 7.13.5 - Cada departamento deverá armazenar suas informações classificadas como restritas ou confidenciais em um local previamente autorizado pela área de T.I.;
 - 7.13.6 - Para cada departamento será criada uma área de armazenamento para compartilhamento de arquivos, de tal forma que os arquivos que possam

- ser compartilhados com outras unidades gerenciais sejam depositados nesta pasta específica;
- 7.13.7 - Deverá ser observada a classificação da informação antes de armazená-la na rede (arquivos públicos podem ser armazenados em locais públicos, arquivos restritos ou confidenciais só poderão ser armazenados em locais restritos);
- 7.13.8 - A permissão padrão para todos os usuários nas pastas de compartilhamento público é de somente leitura;
- 7.13.9 - Cada departamento é responsável pelo tempo de vida da informação arquivada no servidor de arquivos e exclusão de arquivos desnecessários aos interesses da FADISP;
- 7.13.10 - A pasta pública do servidor de arquivos, deverá ser usada somente para arquivos temporários;
- 7.13.11 - Arquivos da pasta pública que com mais de 90 dias sem modificações serão apagados, para liberação de espaço no servidor de arquivos;
- 7.13.12 - Alteração de permissões em qualquer conteúdo deverá ser formalmente autorizada pela área de T.I. em conjunto com a área responsável pela informação, via ferramenta de chamados da área de T.I.;
- 7.13.13 - A gerência de T.I. pode, a qualquer momento, autorizar a inspeção do conteúdo de qualquer pasta, a fim de eliminar possíveis não-conformidades;
- 7.13.14 - Um registro de log será gerado toda vez que uma das seguintes ações for executada: criar pasta, deletar pasta, renomear pasta, criar arquivo, deletar arquivo, alterar arquivo, renomear arquivo, de tal forma que seja possível auditar tais procedimentos.
- 7.14 - **Backup**
- 7.14.1 - Serão executados backups diários de segunda a sexta-feira. Nos backups diários serão copiados apenas os arquivos criados/modificados desde o último backup realizado;
- 7.14.2 - Serão executados backups semanais, os backups semanais contemplarão todos os arquivos encontrados nos locais de armazenamento, independentemente de sua data de criação ou modificação;
- 7.14.3 - Somente serão feitas cópias dos arquivos armazenados nos locais apropriados. Os arquivos considerados não-conformes não serão copiados nos backups.

7.15 - **Prestadores de Serviços (PJ ou Temporários)**

7.15.1 - A relação entre FADISP e seus Prestadores de Serviços (PJ ou temporários) deve ser de respeito e confiança pautados na ética profissional. Por este motivo o prestador de serviços (PJ ou temporário) deve seguir a Política de Segurança da Informação em todos os seus requisitos para a execução de suas funções. Os usuários que desrespeitarem as regras aplicáveis para prestação de serviços estarão sujeitos às sanções definidas no contrato.

7.15.2 - O contrato dos prestadores de serviços deve, necessariamente, estabelecer que a Política de Segurança da Informação seja cumprida na íntegra, assim como as normas de segurança relacionadas ao escopo da contratação, e ainda, estabelecer as penalidades decorrentes de qualquer violação das regras de segurança definidas.

7.16 - **Penalidades:**

7.16.1 - O usuário que infringir qualquer uma das diretrizes de segurança expostas neste instrumento estará passível sem aviso prévio das seguintes penalidades:

- Bloqueios de quaisquer acessos;
- Retirada do equipamento da rede;
- Advertência verbal e/ou escrita, suspensão ou demissão de acordo com o art.30 do capítulo XIV da CLT.

7.16.2 - Toda infração é comunicada ao superior imediato do infrator e, se necessário, à área de RH, a fim de serem tomadas as devidas providências;

7.16.3 - A área de T.I poderá valer-se da autonomia de gestora da informação para atender ou indeferir pleitos de quaisquer usuários da FADISP, restringindo estes pleitos a interesses profissionais, e se necessário, buscar o aval da Gerência correspondente.