Política de Segurança da Informação – LEPES

1. Objetivos e princípios

1.1. A Política de Segurança da Informação (PSI) do Laboratório de Estudos e Pesquisas em Economia Social (LEPES) tem como objetivo estabelecer as orientações, normas, ações e responsabilidades relativas à proteção da informação custodiada ou de propriedade do LEPES.

1.2. Aplica-se diretamente aos projetos realizados em parceria com a Avançar - Associação de Estudos em Políticas Sociais e com a Infinity.

1.3. A PSI do LEPES busca atender aos princípios de segurança da informação e comunicação (confidencialidade, disponibilidade, integridade e autenticidade) da informação gerada, utilizada, armazenada ou distribuída por projetos e pesquisas conduzidos pelo Laboratório, independentemente do meio em que ela esteja contida.

1.4. A PSI deve ser seguida por todos os usuários dos recursos do LEPES para a proteção dos ativos de informação e a prevenção de responsabilidade para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas e/ou equipes do Laboratório.

1.5. A PSI do LEPES é regida pelos preceitos constitucionais, legislação brasileira vigente e pelas normas nacionais e regulamentos do Laboratório. É também regida pelo arcabouço normativo da Universidade de São Paulo.

1.6. Aplica-se, na medida da necessidade, ao ciclo de vida da informação no Laboratório conforme requisitos estabelecidos por seu responsável, proprietário ou plano de gestão de dados.

2. Responsabilidades

2.1. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores e pesquisadores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Todos devem assinar um termo de responsabilidade (Anexo I).

2.2. A PSI deve ser implementada por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função no LEPES, bem como de vínculo empregatício ou prestação de serviço.

2.3. É obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu líder de equipe sempre que não estiver absolutamente seguro quanto ao uso da informação e/ou de ativos e/ou sistemas de informação.

2.4. Todo e qualquer incidente que afete a segurança da informação deverá ser comunicado à Administração do LEPES, que deverá informar a Coordenação.

2.5. Um plano de contingência e a continuidade dos principais sistemas e serviços deverá ser implantado e testado no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade de acesso à informação.

2.6. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de responsabilidade do LEPES, 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 privadas da rede, visando assegurar o cumprimento de sua PSI.

2.7. É responsabilidade do colaborador/pesquisador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo Laboratório notificar imediatamente seu gestor direto. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

3. Diretrizes Gerais

3.1 Estrutura

3.1.1. A informação deve ser armazenada, pelo tempo determinado pelo LEPES, parceiros ou legislação vigente, o que for maior, e recuperável quando necessário. O local de armazenamento das informações (físico ou digital) deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

3.1.2. O uso de dispositivos e redes externas de comunicação (Internet, redes privadas, etc.) deve ser controlado por servidores de firewalls, servidores de acesso à internet, servidores de antiSpam, ferramentas de antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

3.1.3. O acesso externo aos sistemas computacionais do LEPES deve ser controlado e restrito aos serviços necessários, mantendo trilhas de utilização (logs) e restringindo–se ao mínimo necessário.

3.1.4. Sistemas aplicativos e scripts desenvolvidos internamente devem ser documentados e controlados quanto às alterações ou correções feitas, com trilhas do que foi feito e guarda segura da biblioteca de códigos fonte. Toda informação necessária para eventual reconstrução dos aplicativos e scripts deve constar de sua documentação.

3.1.4.1. Especificamente para a elaboração de scripts, recomenda-se seguir as boas práticas (Anexo II)

3.1.5. Sistemas aplicativos e scripts desenvolvidos fora do LEPES, de propriedade de terceiros (com licença de uso para a organização), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes, etc.) sob custódia de uma entidade idônea, de comum acordo entre a organização e a empresa fornecedora do software. Tais fontes devem sempre ser atualizadas e verificadas quanto à sua validade e sincronização com a versão em uso no ambiente de produção.

3.1.6. Os colaboradores com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades do Laboratório e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados.

3.1.7. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Os colaboradores/pesquisadores não poderão em hipótese alguma utilizar os recursos do LEPES para fazer o download ou distribuição de software ou dados pirateados.

3.1.8. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio da Administração do LEPES.

3.1.9. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a Administração do LEPES para obter as instruções devidas.

3.1.10. Todos os recursos tecnológicos adquiridos pelo LEPES devem ter imediatamente suas senhas padrões (default) alteradas.

3.1.11. A Administração do LEPES deve comunicar à Seção Técnica de Informática (STI-FEARP) qualquer incidente relacionado aos equipamentos com patrimônio da Universidade de São Paulo sob responsabilidade do LEPES.

3.2. Gestão

3.2.1. É proibido o compartilhamento de login e/ou senha para funções de administração e acesso aos sistemas. Se existir login e/ou senha de uso compartilhado por mais de um colaborador, a responsabilidade perante ao LEPES será dos usuários que dele se utilizarem.

3.2.2. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o setor administrativo deverá tomar as devidas providências. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado.

3.2.3. A geração, utilização, armazenamento, manutenção, distribuição e destruição dos dados e informações devem ser feitas de acordo com as necessidades do Laboratório, sendo que estes processos devem estar devidamente documentados.

3.2.4. A remessa de dados do Laboratório, seja para atender requisitos do estudo ou pesquisa, como para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos e pela adoção de procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores responsáveis pela informação.

3.3. Propriedade intelectual

3.3.1. As informações produzidas por todos os membros (colaboradores e prestadores de serviço no exercício de suas funções) para o Laboratório, são patrimônio intelectual do LEPES e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o reconhecimento de autoria.

3.4. Papéis

A governança em segurança da informação no LEPES envolve, minimamente, os seguintes atores e responsabilidades principais.

3.4.1. Coordenação

Responsáveis pela gestão do LEPES e, neste caso específico, pela aprovação e publicação da Política de Segurança da Informação.

3.4.2. Administração

Responsáveis pela gestão administrativa do LEPES (contratos, prestação de contas, etc.)

3.4.3. Responsável por ativo de informação

Equipe de dados, responsável por realizar os tratamentos (limpeza, organização, pseudo anonimização) e zelar pela segurança (ou, realizar a proteção) de ativo de informação em uso, ou armazenado.

3.4.4. Usuário da informação

Qualquer pessoa que por força de vínculo com o LEPES tenha necessidade de acesso ou uso de ativo de informação custodiado ou de propriedade do Laboratório.

3.4.5. Parceiro externo

Qualquer pessoa (sem vínculo formal, ou com vínculo temporário) que faça acesso a informação ou serviços disponibilizados por meio recursos de Tecnologia da Informação do LEPES, ou que acesse ou use as instalações físicas do Laboratório.

4. Diretrizes Específicas

4.1. O acesso a softwares peer-to-peer (eMule, Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios online, canais de broadcast e afins) serão permitidos.

4.2. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

4.3. É proibido o uso de computadores e recursos tecnológicos do LEPES para hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

4.4. É de responsabilidade da LEPES publicar e revisar o plano de resposta a incidentes. Esse plano deve conter cada etapa de cada tratativa a partir da identificação de um incidente. Seu objetivo é criar uma abordagem e conduta, minimamente necessária, em caso de um incidente cibernético no Laboratório.

5. Aprovação e atualização da PSI

5.1. Os controles de segurança da informação devem ser planejados, aplicados, implementados e, periodicamente, avaliados de acordo com os objetivos institucionais e os riscos para o LEPES.

5.2. Alteração da PSI do LEPES ou de seus instrumentos derivados será realizada extraordinariamente sempre que identificada a necessidade.

5.3. As modificações e atualizações devem ser aprovadas pela Coordenação do LEPES e estarem em conformidade com as regulamentações da Universidade de São Paulo.

Repositório de procedimentos - https://rpubs.com/lepes_dados