Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

CENTRO UNIVERSITÁRIO PROCESSUS
Prática Extensionista

1. PROJETO (2024.1)

2. 1. <u>Identificação do Objeto</u>

Atividade Extensionista:

( ) PROGRAMA
(x) PROJETO
( ) CURSO
( ) OFICINA
( ) EVENTO
( ) PRESTAÇÃO DE SERVIÇOS
( ) AÇÃO DE EXTENSÃO SOCIAL

Área Temática: Direitos Humanos

Linha de Extensão:

Local de implementação (Instituição parceira/conveniada): Laboratório Júnior de Inovação e Tecnologia (DPDF)

Título Geral: Políticas de Segurança de Dados e Privacidade Digital

2. <u>Identificação dos Autor(es) e Articulador(es)</u>

Curso: Direito

Coordenador de Curso: Adalberto Nogueira Aleixo
Articulador(es)/Orientador(es): Prof. Alberto Carvalho Amaral
Aluno(a)/Equipe:

Nome Completo	Curso / Matrícula	Telefone
Izabela Santos de Queiroz	Direito/ 2323180000010	(61) 98483-2227
Danilo Macedo Alexandrino de Souza	Secretariado/ 2410930000003	(61) 99967-5739
Thiago Ribeiro Wagner	Direito/ 2323180000025	(61) 99954-5771

João Pedro Sharma Rodrigues	Direito/ 2323180000144	(61) 99690-3439
Caio Maia de Souza	Secretariado/ 2310930000032	(61) 99222-7915
Oscar Filipe Melo Maciel	Direito: 2323180000037	(61) 97403-8622
Aurea de Souza Rodrigues	Direito/ 2323180000053	(61) 99203-5822

3. Desenvolvimento

Apresentação:

As políticas de segurança de dados e privacidade digital são diretrizes essenciais para proteger nossas informações pessoais e confidenciais online. Elas garantem que nossos dados, como nome, endereço e informações de contato, sejam mantidos em segurança e não sejam acessados por pessoas não autorizadas. Isso é feito através de medidas como criptografia, controle de acesso e transparência sobre como nossos dados são usados. No entanto, enfrentamos desafios constantes devido à rápida evolução da tecnologia, o que requer atualizações regulares e adaptação para manter nossas informações protegidas contra ameaças digitais.

Fundamentação Teórica:

As políticas de segurança de dados e privacidade digital são fundamentadas na ideia de que nossas informações pessoais devem ser protegidas quando usamos a internet e outros dispositivos digitais. Imagine que suas informações são como segredos guardados em um cofre. Essas políticas são como as regras que garantem que ninguém possa abrir o cofre sem sua permissão e que ele seja mantido seguro o tempo todo. Elas são importantes porque nos protegem de pessoas ou empresas que podem tentar usar nossos segredos de maneiras que não queremos.

Quando esses princípios são seguidos, podemos confiar que nossas informações estão sendo tratadas com respeito e segurança. No entanto, existem desafios, como empresas que tentam coletar mais informações do que precisam ou que não protegem nossos dados adequadamente. Por isso, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, estabelece um conjunto de princípios fundamentais que devem ser observados no tratamento de dados pessoais. Entre esses princípios, destacam-se a finalidade, a adequação, a necessidade e a transparência. A finalidade refere-se ao uso dos dados para propósitos específicos, explícitos e legítimos, enquanto a adequação exige que o tratamento dos dados seja compatível com a finalidade informada ao titular. Já a necessidade impõe a limitação do tratamento ao mínimo necessário para a realização das suas finalidades, e a transparência assegura aos titulares o direito de obter informações claras e acessíveis sobre o tratamento de seus dados. Esses princípios garantem que o tratamento de dados pessoais seja realizado de forma ética e responsável, protegendo os direitos dos titulares.

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

Tema Geral:
Políticas de Segurança de Dados e Privacidade Digital

Tema Específico do Grupo:
Proteção de Dados em Dispositivos

Problema verificado:
Um problema significativo no campo da proteção de dados em dispositivos é a vulnerabilidade à exploração de falhas de segurança em sistemas operacionais e aplicativos. A exploração nas brechas de segurança para acessar dados pessoais.

Objetivo geral:
Promover a educação e a conscientização dos usuários sobre práticas seguras de gerenciamento de dados é outro objetivo vital. Informar os usuários sobre a importância de utilizar senhas fortes, implementar autenticação multifatorial e reconhecer tentativas de phishing pode significar reduzir a probabilidade de comprometimento de dados. Programas de educação em segurança digital, tanto em contextos escolares quanto corporativos, podem equipar indivíduos com o conhecimento necessário para proteger suas informações. Além disso, campanhas de sensibilização pública podem ajudar a criar uma cultura de segurança, onde a proteção de dados seja vista como uma responsabilidade compartilhada entre todos os usuários de tecnologia.

Objetivos específicos:

- Promover palestras;
- Entregar folders impressos explicando ao público o tema abordado;
- Conscientizar a população quanto a importância de serem mantidos em segurança nossos dados pessoais, para que não sejam acessados por terceiros.

Justificativa:

A abordagem das políticas de segurança de dados e privacidade digital justifica-se pelo crescimento exponencial do volume e da sensibilidade dos dados digitais que são coletados, armazenados e processados na sociedade, este cenário tem assustado indivíduos, organizações e governos, devido às frequentes violações de dados e ao uso inadequado de informações pessoais.

No Aspecto social, as políticas de segurança de dados e privacidade digital são fundamentais para proteger a identidade e os direitos dos indivíduos. Com o aumento

dos cibercrimes, como fraudes e roubo de identidade, a proteção dos dados pessoais tornou-se uma prioridade urgente. Incidentes de violação de dados podem causar danos irreparáveis à reputação de empresas e governos, além de consequências financeiras e emocionais para os indivíduos afetados. Essas políticas também são essenciais para garantir a conformidade com leis e regulamentações que visam proteger a privacidade dos cidadãos, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) é uma lei implementada pela União Europeia em 2018, A implementação rigorosa dessas normas promove um ambiente digital mais seguro e confiável, estimulando a inovação e o crescimento econômico enquanto protege os direitos dos cidadãos.

No Aspecto acadêmico, a importância das políticas de segurança de dados e privacidade digital é igualmente crucial. Instituições de ensino e pesquisa lidam com uma quantidade de dados sensíveis, incluindo informações pessoais de estudantes, pesquisadores e funcionários, bem como dados de pesquisas científicas, As universidades e escolas também enfrentam desafios relacionados à segurança cibernética, como a proteção contra ataques de hackers que podem comprometer dados de pesquisa valiosos ou causar interrupções nos sistemas educacionais. Além disso, a privacidade digital é essencial para garantir um ambiente de aprendizado seguro, onde os estudantes possam interagir e colaborar sem medo de que suas informações pessoais sejam expostas ou utilizadas de maneira inadequada.

Quanto às sanções, o não cumprimento das disposições estabelecidas pela LGPD pode resultar em penalidades severas para os responsáveis pelo tratamento dos dados. As sanções administrativas, aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), incluem advertência, multa simples ou diária, e até mesmo a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados. A multa pode atingir até 2% do faturamento da empresa no seu último exercício, limitada a R$50 milhões por infração. Além disso, a publicização da infração pode ser determinada, após devidamente apurada e confirmada a sua ocorrência, como forma de promover a transparência e a accountability. Estas penalidades são mecanismos que visam garantir a conformidade com a LGPD e proteger os direitos dos titulares de dados pessoais.

Metas: Instruir o público-alvo acerca de como se proteger, protegendo seus dados pessoais, e consequentemente a não infringir os de outras pessoas, tornando assim a internet que é uma das ferramentas mais utilizadas ultimamente um local mais seguro e sem riscos pros usuários.

Hipótese / Resultado esperado:
Que tomem ciência sobre o tema apresentado e acabam sendo mais cautelosos ao entrar em determinados sites, sabendo que suas informações pessoais podem estar em jogo com qualquer clique falso.

Metodologia:

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

Entregar folders para os cidadãos que vão estar presentes na Praça do Relógio e falar um pouco da importância do nosso tema.

Cronograma de execução:

Data de início: 1 de março de 2024

Data de término: 1 de julho de 2024

Evento	Período	Observação
Definição do Tema	06 a 12/04/24	
Pesquisa Bibliográfica	13 a 26/04/24	
Visita Técnica DPDF	12/04/24	
Elaboração do Formulário de Pesquisa	27/04 a 02/05/24	
Elaboração do Projeto	04 a 09/05/24	
Elaboração do Panfleto	10 a 23/05/24	
Apresentação do Pré-Projeto	24/05/24	
Ação junto à comunidade - Entrega de panfletos	25/06 a 27/06	
Entrega do projeto Final	27/06/24	
Entrega de panfletos na Praça do Relógio/ Estação de Metrô	27/06/2024	Praça do Relógio Estação de Metrô
Elaboração do Relatório Final	27/06 a 30/06/24	
Apresentação do Relatório Final	01/07/24	

Referência Bibliográfica:

Privacidade e Proteção de Dados Pessoais: Comentários à Lei nº 13.709/2018 - LGPD - Camara, E. P. (2020).

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

Segurança Digital: Práticas Essenciais para Proteger Informação e Comunicação - Filho, L. C. C. (2019).

Cibersegurança: Como Proteger Seu Negócio Contra Ataques - Freitas, M. A. (2018).