Equipe:

Nome: Felipe Morais Carrapeiro – RM:84507

Seção II – Tratamento de Dados Pessoais Sensíveis:

Obtenção e Gerenciamento de Consentimento:

A startup obterá o consentimento explícito dos usuários antes de coletar qualquer dado sensível, fazendo com que uma nova interface deverá ser desenvolvida explicando de forma detalhada como os dados serão utilizados, possuindo a existência do usuário revogar esse consentimento a qualquer momento.

Segurança de Dados Sensíveis:

Contando que a Seção II da LGPD inclui informações sobre a saúde e outros dados que são considerados de alta criticidade, mesmo com o WebApp não coletando diretamente informações de saúde, a monitoração de situações de risco à segurança de idosos pode envolver o tratamento de informações sobre a condição física dos usuários. Por conta disso será garantido que somente a pessoa responsável pelo idoso receberá o chamado de ajuda.

Por conta de o WebApp lidar com dados críticos em tempo real (sendo os alertas de incêndio, vazamento de gás ou queda), que acabam exigindo um alto nível de proteção e confiabilidade, a orientação da Seção II da LGPD é crucial para assim necessário o consentimento do usuário e possuir uma segurança adequada para evitar possíveis acessos indesejados.

Embora as senhas não sejam necessariamente classificadas como dados sensíveis de acordo com a LGPD, elas acabam sendo informações críticas para a segurança dos dados dos usuários, e para caso o banco de dados seja comprometido as senhas são armazenadas utilizando hashing e salt para que as senhas não sejam facilmente expostas.

Transparência e Finalidade:

A startup garante que está coletando somente os dados necessários para fornecer o serviço, evitando a coleta de informações desnecessárias. Será criado uma política de privacidade acessível e clara, informando detalhadamente como os dados serão utilizados.

Plano de Resposta e Incidentes:

Por conta de serem funções e soluções eficientes para a proteção dos dados e da segurança dos usuários acaba sendo bem difícil de acabar acontecendo algum descumprimento com a Seção da LGPD escolhida, o que resultaria em quase nenhum impacto financeiro negativo na startup, porém caso ocorra algum descumprimento, a pessoa lesada possuirá um suporte para sanar qualquer insatisfação, e imediatamente a ANPD será notificada sobre o ocorrido, incluindo: uma descrição da natureza dos dados afetados; informações sobre o responsável pelo tratamento; medidas técnicas e de segurança adotadas para a proteção dos dados; riscos relacionados ao incidente; medidas tomadas ou que serão tomadas para mitigar os efeitos. Além de notificar a ANPD deverá ser alinhado quais multas devem ser pagas, sendo que o valor destas multas podem chegar a até 2% do faturamento anual da empresa.

Política de Segurança:

Algumas das políticas a serem tomadas já foram explicadas anteriormente, porém para se aprofundar mais terão mais alguns tópicos abaixo.

Armazenamento e destruição dos dados:

Os dados já estão sendo armazenados em um banco não relacional, sendo ele o Mongodb, como dito anteriormente os dados sensíveis possuem criptografia e todos os dados possuirão backup que serão realizados periodicamente para assim garantir a integridade e disponibilidade das informações caso o sistema falhe.

Na parte de destruição dos dados, todo usuário que não tiver um tempo de atividade mínimo de 3 anos terá todos seus dados excluídos de forma irreversível. Outra forma de os dados do usuário serem excluídos de forma irreversível é caso o mesmo entre em contato com o suporte e solicite a remoção de suas informações.

Recomendações de Segurança:

No WebApp possuirá validação de senhas para que sejam mais seguras, obrigando o usuário a possuir uma senha com mais de 8 caracteres e possuindo pelo menos uma letra maiúscula e caractere especial.

Será implementado um fator de MFA para que o usuário possua uma forma de autentificação multifator e assim ter mais segurança sobre sua conta.

O usuário receberá em seu email mais sugestões de segurança para evitar possíveis riscos com a integridade de seus dados, sendo informado que suas informações confidenciais não devem ser compartilhadas, e caso seja realmente necessário compartilhar, que seja por canais seguros.