Preocupações de Desenvolvedor de aplicações móveis com a Segurança

Como desenvolvedor de aplicações móveis gostaríamos de lhe convidar para compartilhar a sua opinião conosco sobre aspectos de segurança baseados na norma **ISO 27002**. Esta norma funciona como um código de práticas que auxilia na aplicação de um Sistema de Gestão da Segurança da Informação.

Nossa pesquisa é de cunho acadêmico, desenvolvida no contexto de um Trabalho de Conclusão de Curso no Bacharelado em Sistemas de Informação da PUCRS, e sem fins comerciais. Sua participação é voluntária e sua opinião será anônima e confidencial. Você pode desistir de participar da pesquisa a qualquer momento e pedir que desconsideremos suas respostas mesmo que parciais.

O tempo de preenchimento estimado do questionário é de aproximadamente **15 min.** Agradecemos a sua colaboração! Será um prazer compartilhar os resultados consolidados e nosso aprendizado com este estudo caso seja de seu interesse. Basta indicar ao final do questionário que deseja recebê-los.

Equipe de pesquisa PUCRS:

- Vinicius Jaggi (aluno de graduação em Sistemas de informação, PUCRS) - vinicius.jaggi@edu.pucrs.br

- Caio Borges (aluno de doutorado em Ciência da Computação da PUCRS) - caio.borges@acad.pucrs.br

- Azriel Majdenbaum (professor da Escola Politécnica da PUCRS, orientador) -azriel.majdenbaum@pucrs.br

- Sabrina Marczak (professora da Escola Politécnica PUCRS, co-orientadora) - sabrina.marczak@pucrs.br

controle de acesso

Por favor, indique o seu grau de concordância o u discordância com as afirmativas abaixo. Use a escala de 1 a 5: sendo que 1 indica "discordo totalmente" e 5 indica "concordo totalmente".

Questão 1. Segundo a ISO 27002, um **controle de acesso** tem como objetivos limitar o acesso à informação e aos recursos de processamento da informação, assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas, serviços e aplicações. Este controle pode ocorrer de diferentes formas, por exemplo, através de uma senha de acesso ou controle de sessões do sistema.

1.1

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me com o controle de acesso de usuários nos sistemas que desenvolvo.	○	○	○	○	○

1.2

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em criar ou utilizar funcionalidades que permitam o bloqueio, remoção ou desabilitação rápida de usuários no sistema (por exemplo, funcionários que deixaram a empresa).	○	○	○	○	○

1.3

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em desenvolver funções que permitam a alteração de permissão no sistema para todos os usuários, ou seja, que seja possível o gerenciamento de usuários.	○	○	○	○	○

1.4

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em criar um registro central de direitos de acesso para cada usuário, ou seja, todos os usuários possuem um ID único.	○	○	○	○	○

Questão 2. Uma autenticação em um aplicativo móvel tem como objetivo assegurar que um sujeito é realmente quem ele diz ser. Esta autenticação é realizada, em geral, baseada em algum dado de identificação (por exemplo, uma senha, um token, uma impressão digital) e é referida pela ISO 27002 como **autenticação secreta**.

2.1

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em desenvolver funções que verifiquem a identidade de um usuário antes de fornecer uma informação de autenticação secreta, temporária, de substituição ou nova no sistema. (por exemplo e-mail de confirmação, SMS, aplicativos como Google autenticador).	○	○	○	○	○

2.2

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em aprimorar o desenvolvimento de funcionalidades com autenticação secreta para acessos e logins. (autenticação por 2 fatores).	○	○	○	○	○

2.3

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me para que a Informação de autenticação secreta temporária seja única para uma pessoa e que não possa ser facilmente adivinhada.	○	○	○	○	○

2.4

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em fornecer recursos para que o usuário consiga resguardar sua privacidade durante o processo de autenticação.	○	○	○	○	○

2.5

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em não mostrar dados sensíveis do usuário (status, informações pessoais, etc.) de aplicações até que o processo de Log-on tenha sido concluído com sucesso.	○	○	○	○	○

2.6

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em validar informações de entrada no sistema somente quando todos os dados de entrada estiverem completos.	○	○	○	○	○

2.7

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Caso ocorra um erro na validação das informações de entrada me preocupo em não identificar qual parte do dado de entrada está correto ou incorreto (Ex: "Sua senha está incorreta").	○	○	○	○	○

2.8

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em proteger o sistema contra tentativas consecutivas/repetidas de entrada forçada.	○	○	○	○	○

2.9

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em comunicar um evento de segurança caso uma tentativa potencial ou uma violação bem sucedida de entrada no sistema (log-on), seja detectada.	○	○	○	○	○

2.10

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em encerrar sessões inativas após um período de inatividade.	○	○	○	○	○

2.11

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em fazer sistemas que obriguem uma escolha de senha de qualidade, por exemplo, com no mínimo Oito Caracteres, misturar letras em caixa alta e baixa com números e caracteres não alfanuméricos).	○	○	○	○	○

2.12

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em desenvolver sistemas que obriguem usuário a mudarem as suas senhas temporárias no primeiro acesso ao sistema (Sistema que coloca sua senha inicial como data de aniversário ou dígitos do RG).	○	○	○	○	○

2.13

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em não permitir que a senhas possam ser mostradas na tela quando digitadas (Ex: Usar recurso do “olho” para revelar senha em um campo).	○	○	○	○	○

Criptografia

Por favor, indique o seu grau de concordância/discordância com as afirmativas abaixo. Use a escala de 1 a 5: sendo que 1 indica “discordo totalmente” e 5 indica “concordo totalmente”.

Questão 3. Segundo a ISO 27002, a **Criptografia** tem como objetivo assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e a integridade da informação.

3.1

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me com uso de criptografia para a proteção das informações sensíveis durante a comunicação em dispositivos móveis.	○	○	○	○	○

3.2

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em gerar chaves para diferentes sistemas criptográficos e diferentes aplicações.	○	○	○	○	○

Segurança nas operações

Por favor, indique o seu grau de concordância/discordância com as afirmativas abaixo. Use a escala de 1 a 5: sendo que 1 indica “discordo totalmente” e 5 indica “concordo totalmente”.

Questão 4. A **segurança das operações** tem como objetivos: (*i*) garantir a operação segura e correta dos recursos de processamento da informação; (*ii*) assegurar que as informações e os recursos de processamento da informação estão protegidos contra *malware*; (*iii*) a proteção contra perda de dados; (*iv*) registrar eventos e gerar evidências; (*v*) assegurar a integridade dos sistemas operacionais, e; (*vi*) prevenir a exploração de vulnerabilidades técnicas e minimizar o impacto das atividades de auditoria nos sistemas operacionais.

4.1

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me com os impactos na segurança da informação quando ocorre alguma mudança no sistema.	○	○	○	○	○

4.2

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em criar mecanismos para atender o crescimento da aplicação e possibilitar suportar demanda variável de acessos.	○	○	○	○	○

4.3

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me para que dados sensíveis não sejam copiados para os ambientes de testes.	○	○	○	○	○

Questão 5. Em relação a registros de eventos (logs), por favor, responda as questões a seguir:

5.1

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em criar mecanismos para registrar os eventos do sistema.	○	○	○	○	○

5.2

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me com datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (log-on) e saída (log-off) no sistema.	○	○	○	○	○

5.3

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me com a identificação do dispositivo ou sua localização quando possível e o identificador do sistema.	○	○	○	○	○

5.4

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me com registro de tentativas de acesso ao sistema, aceitas e rejeitadas.	○	○	○	○	○

5.5

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me com a coleta dos endereços e protocolos de rede no log.	○	○	○	○	○

5.6

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me para que arquivos de log não sejam editados ou excluídos sem a devida autorização.	○	○	○	○	○

Aquisição, desenvolvimento e manutenção de sistemas.

Por favor, indique o seu grau de concordância/discordância com as afirmativas abaixo. Use a escala de 1 a 5: sendo que 1 indica “discordo totalmente” e 5 indica “concordo totalmente”.

Questão 6. A **Aquisição, desenvolvimento e manutenção de sistemas** tem como objetivo garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação, garantir que

a segurança da informação esteja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação e assegure a proteção dos dados usados para teste.

6.1

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em identificar falhas de segurança nas aplicações móveis que dou manutenção.	○	○	○	○	○

6.2

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me para que as informações envolvidas nos serviços de aplicação que transitam em redes que são de acesso público sejam protegidas de atividades fraudulentas, disputas contratuais e divulgações e modificações não autorizadas.	○	○	○	○	○

6.3

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em usar protocolos de comunicação seguros para obter uma transação segura e confidencial.	○	○	○	○	○

6.4

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em evitar que os detalhes da transação fiquem em um meio de armazenamento acessível diretamente pela internet, sem a devida segurança.	○	○	○	○	○

6.5

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em utilizar repositórios seguros para construção de aplicações.	○	○	○	○	○

6.6

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me com a análise dos controles da aplicação e dos procedimentos de integridade para assegurar que eles não tenham sido comprometidos pelas mudanças na plataforma operacional.	○	○	○	○	○

6.7

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em analisar novas tecnologias para serem aplicadas para reduzir os riscos de segurança.	○	○	○	○	○

6.8

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em analisar os riscos (impacto/probabilidade) para prover o desenvolvimento de segurança na aplicação.	○	○	○	○	○

6.9

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em separar diferentes ambientes de desenvolvimento (dev/ teste /prod).	○	○	○	○	○

6.10

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me com a sensibilidade dos dados a serem processados, armazenados e transmitidos pelo sistema.	○	○	○	○	○

6.11

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em realizar testes de segurança em funcionalidades desenvolvidas.	○	○	○	○	○

6.12

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em realizar testes unitários.	○	○	○	○	○

6.13

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em realizar testes das funcionalidades desenvolvidas, de maneira integrada no sistema.	○	○	○	○	○

6.14

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em utilizar ferramentas de análise de código.	○	○	○	○	○

6.15

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em realizar testes de aceitação de sistemas.	○	○	○	○	○

6.16

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em cuidados dos dados de testes, caso o banco de dados operacional seja utilizado.	○	○	○	○	○

6.17

	Discordo totalmente	Discordo	Não estou decidido	Concordo	Concordo totalmente
Preocupo-me em proteger os dados do banco de dados operacional contra remoção e modificação.	○	○	○	○	○

SOBRE VOCÊ

Nos conte um pouco sobre você, por favor.

1.Quais das plataformas abaixo tens experiência?

Selecione uma ou mais opções

- [ ] Android: Kotlin
- [ ] Android: Java
- [ ] iOS: Swift
- [ ] iOS: Objective-C
- [ ] Android: Web application
- [ ] iOS: Web Application
- [ ] Android: Flutter/DART

2. Quantos aplicativos móveis em média você desenvolveu nos últimos 3 anos?

3. Há quantos anos você vem desenvolvendo aplicativos móvel?

4. Você geralmente desenvolve aplicativos móvel em equipe?

- ○ Não, eu geralmente desenvolvo sozinho
- ○ Sim, eu geralmente desenvolvo em equipe
- ○ Eu nunca desenvolvi um aplicativo móvel antes

Quais tipos de contribuição você costuma realizar?

- ☐ Desenvolver aplicativos para a loja de aplicações do ecossistema
- ☐ Desenvolver aplicativos de uso empresarial (B2B)
- ☐ Desenvolvo aplicativos de forma livre (indie)
- ☐ Desenvolvo aplicativos open-source.

CONCLUINDO

Click to write the question text

1. Você gostaria de deixar algum comentário adicional sobre o assunto de segurança em aplicativos móvel?

2. Você gostaria de receber uma cópia do nosso relatório com os resultados consolidados desta survey?

- ○ Sim, eu gostaria de receber
- ○ Não, obrigado

3. Por favor, deixe seu e-mail para lhe enviarmos o relatório

Muito obrigado por sua participação!