POLÍTICA DE SEGURANÇA DA INFORMAÇÃO GLOBAL

IATec
Instituto Adventista de Tecnologia

1. OBJETIVO

Esta Política tem como objetivo estabelecer as diretrizes de Segurança da Informação para o estabelecimento do IATec (Instituto Adventista de Tecnologia), e responsabilidades para promover a confidencialidade, integridade e disponibilidade das informações na organização.

A política de segurança da informação foi elaborada considerando os requisitos derivados de:

a. Estratégia e requisitos de negócios;
b. Regulamentações, legislação e contratos;
c. Riscos e ameaças atuais e projetados para a segurança da informação.

2. PÚBLICO-ALVO

Esta política aplica-se a todos os usuários, colaboradores, prestadores de serviços, fornecedores e clientes do IATec, que acessam informações, estejam elas armazenados nas instalações físicas, nos parceiros de negócios ou em dispositivos pessoais e/ou de propriedade do IATec, tais como celulares, tablets, desktop, notebooks, IoT ou qualquer outro recurso computacional.

3. TERMOS E DEFINIÇÕES

• **Alta Direção:** Diretoria Executiva composta pelo Diretor Geral (CEO), Diretor Financeiro (CFO) e Diretor Técnico (CIO) do IATec.
• **Gestores:** gerentes responsáveis por assegurar a condução adequada das atividades do dia a dia do IATec. ● Colaboradores: profissionais que prestam serviço de forma direta ao IATec. Exemplos: membros de comissões, membros dos comitês, empregados, obreiros, temporários, estagiários e terceiros. ● Fornecedores: empresas/pessoas jurídicas que fornecem produtos e/ou serviços para o IATec. ● Prestadores de Serviço e Parceiros: empresas/profissionais externos ao IATec e que prestam serviços por meio de contrato específico.
• **Terceiros:** mão-de-obra profissional que presta serviço de forma contínua ao IATec por meio de empresa intermediadora. Exemplos: (Consultores, Desenvolvedores e Vigilantes).
• **Usuário**: toda pessoa, seja religioso, obreiro, missionário, empregado ou equiparado, voluntário, prestador de serviços, remunerado ou não, habilitado e/ou autorizado por meio da assinatura de Termo de Responsabilidade, Ciência e Compromisso, quando aplicável, a acessar os Recursos de Informática e Comunicação de Dados ou ativos de informação do IATec ou de outras entidades da Igreja Adventista do Sétimo Dia.
• **Comitê de Segurança da Informação e Proteção de dados (CSIPD):** órgão permanente do IATec, responsável pela discussão e definição de diretrizes envolvendo riscos e temas técnicos de segurança da informação e privacidade. O órgão é composto pelo Diretor Técnico e pelos líderes das gerências técnicas de Inovação, Desenvolvimento, Privacidade/Jurídico, Infraestrutura e Segurança da Informação.

• **Segurança da Informação**: A área de segurança da informação no IATec é responsável pela resposta a incidentes, garantir o ciclo de desenvolvimento seguro, identificar vulnerabilidades, promover conscientização e neutralizar ameaças cibernéticas. O termo "segurança da informação" refere-se à confidencialidade, integridade, disponibilidade da informação.

4. REFERÊNCIAS

- Este documento foi elaborado com base nos seguintes documentos de referência:
- Código de Prática para controles de segurança da informação – ISO/IEC 27002;
- Framework for Improving Critical Infrastructure Cybersecurity – NIST;
- Center for Internet Security – CIS Controls;
- ISF Security Foundation Framework;

5. DISPOSIÇÕES GERAIS

5.1. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

a. A gerência responsável pela Segurança da Informação do IATec é a área de Segurança da Informação.
b. A Diretoria Executiva e a área de Segurança da Informação devem discutir e aprovar a estratégia de segurança da informação do IATec visando melhoria contínua do sistema de gestão de segurança da informação.
c. Há um CSIPD constituído que se reune periodicamente para avaliar, discutir e definir ações de tratamento dos riscos de segurança da informação.
d. O IATec promove boas práticas em Segurança da informação no seu ambiente corporativo. A conscientização deve ser realizada por ambas as partes: contratada e contratante.
e. As diretrizes de segurança da informação devem ser compartilhadas com todas as partes interessadas do IATec.

5.2. CONTROLE DE ACESSO

a. Para a utilização de todo e qualquer serviço ou sistema ou para o acesso a documentos físicos do IATec será necessária a dupla intencionalidade: legitimidade do cargo e interesse. Ao envolver Tecnologia da Informação (rede, sistemas, correio eletrônico e demais serviços), será necessário que os seus usuários se identifiquem através de credenciais previamente cadastradas e devem ter interesse legitimo na execução da sua atividade.
b. Ainda assim, para desempenhar suas funções, o prestador, parceiro ou cliente deve possuir acesso aos recursos inerentes à sua atividade limitados à sua função, baseado em análise de riscos, segregação de funções e o nível de classificação da informação acessada.

c. A gestão dos acessos básicos e recursos de informática e comunicação do IATec para prestadores ou parceiros é administrada pela área de Segurança da Informação. As demandas para criação, alteração e/ou revogação destes acessos devem ser realizadas mediante solicitação via e-mail/chamado, principalmente após comunicado do encerramento do vínculo contratual, assim como quaisquer licenciamentos associados aos respectivos usuários. Cabendo à Diretoria Executiva, analisar ressalvas em situações específicas com o devido alinhamento das áreas de Segurança da Informação e Jurídica.
d. As senhas de usuários individuais não devem ser compartilhadas. Seu uso é restrito e pessoal sendo a divulgação considerada como violação desta política de segurança. No entanto, para garantir que os acessos estejam em conformidade, ou assegurar a integridade das senhas, haverá uma revisão de acessos e troca de senha semestralmente. A fim de tornar a segurança da informação um hábito no cotidiano do usuário, serão feitas ações educativas concomitantes a revalidação de acessos.
e. O acesso dos sistemas e aplicações do IATec para prestadores ou parceiros são autorizados e provisionados pelos gerentes/líderes de área, após triagem das solicitações pela área de Segurança da Informação.
f. Todo e qualquer acesso provisionado aos sistemas e recursos de informática e comunicação do IATec para prestadores ou parceiros deve ser solicitado de maneira formal, mediante aprovação de gerente/líder imediato e gestor do ativo. Os acessos concedidos devem ser revisados periodicamente.
g. Os acessos de prestadores de serviço para qualquer nível de informação ou até mesmo um acesso privilegiado devem ser concedidos mediante solicitação dos gerentes/líderes das áreas com o aval da Segurança da Informação, com data de acordo com a vigência e finalidade do contrato, devendo ser revogados após o término da vigência do mesmo. Ou seja, nenhum prestador de serviço pode ter acesso sem assinatura de contrato de prestação de serviços. Deve ser observado junto ao departamento jurídico enquadramento de cláusulas de sigilo, acordos de não divulgação (NDA), orientações de privacidade e segurança para o prestador de serviço regidas em contrato.
h. O acesso aos códigos-fonte de sistemas e aplicações do IATec deve ser restrito a prestadores ou parceiros autorizados, mediante aprovação formal alinhada com a área de Segurança da Informação.

5.3. SEGURANÇA DE DADOS E INFORMAÇÕES DA ORGANIZAÇÃO

O IATec disponibiliza recursos de informática e comunicação aos prestadores, parceiros e usuários autorizados de modo a auxiliá-los no desempenho de suas atividades.
a. Os acessos são monitorados, e os registros são armazenados por período determinado de acordo com leis em vigência e de uso exclusivo do IATec.
b. A conta de e-mail corporativa quando disponibilizada pelo IATec não deve ser utilizada para fins de cadastro em ferramentas externas como sites de compras, relacionamento pessoal, grupos de interesse, listas ou fóruns públicos, não ligados à respectiva atividade.

c. O Acesso remoto se dará exclusivamente por software de comunicação segura (VPN) previamente autorizada. O IATec possui ambiente controlado para serviços internos, o acesso se dará de forma supervisionada ou através de recurso computacional disponibilizado pelo IATec.
No que diz respeito ao uso das informações digitais ou físicas do IATec, NÃO É PERMITIDO:
d. O acesso, armazenamento, edição, cópia, posse ou distribuição não autorizados, por via eletrônica ou qualquer outro meio, de informações, dados e/ou dados pessoais/confidenciais sob responsabilidade do IATec;
e. O envio de mensagens por e-mail entre quaisquer usuários ou mesmo externamente que contenham vírus ou arquivos maliciosos, contenham material de natureza político-partidária ou sindical;
f. Distribuir ou adquirir software não autorizados e/ou não licenciados;
g. O acesso, armazenamento, edição, cópia, posse ou distribuição com conteúdo pornográfico, ilegal ou quaisquer que estejam em desacordo com os princípios da instituição;
h. Divulgar informações do IATec em comunidades virtuais e redes sociais que exponham a organização ou a Instituição;
i. Infringir os direitos de propriedade intelectual de empresas e/ou terceiros, no que diz respeito a qualquer software, material audiovisual, publicações e demais informações eletrônicas (incluindo plágio e uso ou reprodução não autorizados);
j. Realizar cópias de segurança, de arquivos, documentos físicos ou digitais, dados pessoais de outras pessoas em dispositivos particulares, inclusive em "nuvem" pessoal.
k. Desvio de finalidade do uso dos recursos de informática e comunicação de dados nas atividades desempenhadas.

5.4. USO DE DISPOSITIVOS DE INFORMÁTICA

a. O IATec não disponibiliza o equipamento necessário e acessórios para seus usuários, prestadores ou parceiros.
b. As configurações de segurança do dispositivo de informática, devem ser aplicadas minimamente: I. Utilização de software contra vírus e arquivos maliciosos.
II. Mecanismos de criptografia e backup habilitados.
III. Qualquer aplicação utilizada é necessária o respectivo licenciamento;

5.5. PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

a. Todos os dispositivos de informática (aplicáveis) conectados à rede corporativa do IATec e servidores devem possuir software antivírus licenciado, instalado e atualizado, antes da transferência dos dados para a máquina do usuário ou servidores.
b. A atualização da vacina nos dispositivos de informática (aplicáveis) e servidores deve ser realizada de forma automática, com as respectivas validações periódicas para garantir que nenhum dispositivo esteja desatualizado.

c. Faz parte do protocolo de segurança, verificações (varreduras) periódicas automáticas em todos os dispositivos de informática (aplicáveis) conectados à rede, inclusive periféricos ou acessórios externos. Os servidores também necessitam de software de antivírus licenciado, instalado e atualizado. d. Em caso de detecção de vírus, os arquivos maliciosos identificados devem ser excluídos.

5.6. BYOD/DISPOSITIVOS PARTICULARES

a. Considerando que dispositivos BYOD/particulares não são máquinas que permitem customizações pela TI, o recomendado é que máquinas não gerenciadas pela instituição, não possuam acessos aos serviços abaixo devido a risco de uma possível infecção de softwares maliciosos:
I. Conexão lógica com o segmento de rede de servidores;
II. Compartilhamento de rede com estações de trabalho;
III. VPN conforme item 5.3.c;
IV. Acesso à arquivos corporativos localmente (servidor de arquivos, compartilhamentos, etc.);
V. Filiação ao domínio que gerencia as estações de trabalho (risco de elevação de privilégio);
VI. Aplicação de licenciamento institucional ou colaborativo por chaves, onde não há gestão sobre o recurso.
b. O usuário do dispositivo deve zelar pela integridade da rede, segurança das informações e correto manuseio dos sistemas, mesmo em seus dispositivos particulares/BYOD de acordo com as orientações abaixo: I. Não divulgar informações confidenciais do IATec que estão armazenadas no dispositivo móvel para desconhecidos, a menos que seja necessário (ex.: inspeção em aeroportos).
II. Bloquear a tela do dispositivo quando não estiver em uso.
III. Em viagens aéreas, o dispositivo móvel deve ser carregado como bagagem de mão.
IV. Em aeroportos e locais movimentados como restaurantes, shoppings, lojas e eventos, ficar atento ao dispositivo móvel durante todo o tempo, e durante viagens terrestres, transportar o equipamento no porta-malas.
V. Em caso de execução de atividades profissionais fora das instalações físicas do IATec, guardar o equipamento em local seguro sempre que se afastar do dispositivo de informática.

5.7. GESTÃO DE INCIDENTES

a. A responsabilidade de realizar a gestão de incidentes de segurança da informação do IATec é da área de Segurança da Informação em alinhamento com o departamento jurídico e encarregado de privacidade de dados.
b. O prestador e/ou parceiro deve implementar mecanismos de detecção de incidentes de segurança da informação em seu ambiente de TI que conduzirá, periodicamente, varreduras e análises para identificação de vulnerabilidades de segurança da informação nos sistemas.

c. Os prestadores e/ou parceiro devem reportar inicialmente a área de segurança do IATec qualquer incidente de segurança observado, com o máximo de detalhes possíveis, envolvendo brechas de segurança da informação e/ou o não cumprimento da política e normas do IATec, e legislação aplicáveis.
d. Os incidentes de segurança da informação serão classificados, registrados, tratados e devidamente comunicados. A área de segurança da informação pode, quando na detecção de um incidente de segurança da informação, mitigar o risco e até mesmo, solicitar ao prestador e/ou parceiro investigação da causa raiz.
e. NINGUÉM, exceto aqueles que sejam autorizados pelo IATec, deve pronunciar-se publicamente a respeito de qualquer tipo de incidente de segurança da informação e privacidade de dados que envolva o IATec.
f. Deve ser mantido o histórico do incidente tratado, para ser armazenado em base de conhecimento, de forma que possa ser usado para reduzir a probabilidade ou o impacto de incidentes futuros.
g. O canal de comunicação para relatar incidentes de segurança da informação é security@iatec.com ;

5.8. POLÍTICA DE SENHA

Reitera-se que a senha é pessoal e intransferível conforme detalhado na sessão controle de acesso. Os requisitos de senha utilizados contemplam boas práticas de mercado (Exemplo: CIS Controls, ISO 27000, 27001 e 27002).
Para evitar acessos indevidos, o IATec terá mecanismos de restringir senhas fracas no momento da criação ou alteração. Em caso de suspeita de comprometimento do respectivo login/conta por agentes externos ou terceiros haverá a suspensão automática preventiva do acesso.

5.9. CRIPTOGRAFIA

a. Para garantir a integridade das informações, comunicação segura entre seus ambientes de rede e dispositivos, o IATec proverá recursos e mecanismos de criptografia.
b. Para conexão ao ambiente de rede do IATec quando disponibilizado, devem ser utilizados softwares de VPN com criptografia habilitada.
c. Os dispositivos e serviços utilizados devem possuir mecanismos de criptografia na comunicação. d. Os backups devem ser armazenados em locais seguros, homologado e disponibilizado pelo IATec com mecanismos de criptografia habilitados.

5.10. INTEGRAÇÃO E EXTRAÇÃO DE DADOS

a. A vinculação ou criação de interface de qualquer sistema mantido e homologado pelo IATec com outra aplicação externa, deverá necessariamente ser requisitado para área de Seguran-

ça da Informação do IATec, através do e-mail security@iatec.com , que fará análise inicial e encaminhará para apreciação ao CSIPD do IATec, de modo que nenhum acesso aos bancos de dados ou extração automatizada de relatórios seja feita sem os devidos protocolos de segurança.

5.11. PROPRIEDADE INTELECTUAL

a. A propriedade intelectual deve ser respeitada conforme o respectivo contrato.

5.12. AUDITORIA, RISCOS E CONFORMIDADE

a. O IATec tem prerrogativa de auditar em eventuais necessidades os riscos, vulnerabilidades, medidas de mitigação, nível de maturidade em Segurança da Informação e conformidade desta política em relação aos prestadores e/ou parceiros para garantir aderência com esta política.

6. EXCEÇÕES

As exceções e casos omissos à política e normas de segurança da informação devem ser analisadas pelo CSIPD do IATec, sob a ótica de gestão de riscos de segurança da informação e objetivos estratégicos do IATec. A área de Segurança da Informação deve avaliar os impactos e encaminhará ao Comitê acima para análise e discussão, e posteriormente, apresentar o resultado para aprovação das exceções pela Diretoria Executiva.

7. RESPONSABILIDADES

7.1. USUÁRIOS

a. Compreender e aplicar essa política do IATec;
b. Comunicar casos omissos desta política ao Departamento de Segurança da Informação do IATec;
c. Reportar violações da política e normas a área de Segurança da Informação do IATec.

7.2. GERENTES/LÍDERES

a. Gerenciar o acesso aos prestadores de serviços, observando a concessão de acesso de acordo com a vigência contratual;
b. Dar ciência dessa política de segurança a todos os seus liderados ou prestadores de serviços/terceiros envolvidos com seus respectivos departamentos;

7.3. PRESTADORES DE SERVIÇOS/TERCEIROS/PARCEIROS

a. Compreender e atender plenamente a Política de Segurança da Informação adotada pelo IATec, de acordo com cláusulas de segurança, proteção de dados pessoais, confidencialidade e sigilo assinado no contrato de prestação de serviços.

7.4. COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS DO IATEC - CSIPD

a. Assessorar a implementação das ações de Segurança da Informação do IATec;
b. Discutir casos omissos desta política para verificar a necessidade de revisão do documento;
c. Revisar anualmente, ou sempre que necessário, as propostas de atualização desta política e demais normas de segurança da informação, de acordo com os interesses e objetivos de negócio do IATec, efetuando as alterações necessárias e, em seguida, encaminhando para aprovação da Diretoria Executiva e publicação; d. Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos.

7.5. JURÍDICO

a. Avaliar e revisar contratos de prestação de serviços com as cláusulas de segurança e dados, segurança de dados pessoais e termos de sigilo e confiabilidade.

7.6. SEGURANÇA DA INFORMAÇÃO

a. Acompanhar as investigações em caso de violação da desta política;
b. Acompanhar assuntos relativos à segurança da informação que envolva ao IATec (ex.: novas leis, regulamentos, novas tecnologias, dentre outros);
c. Atuar na divulgação, conscientização e treinamento dos envolvidos, promovendo a cultura de segurança da informação;
d. Responder os incidentes de Segurança da Informação do IATec;
e. Formalizar solicitações e acompanhar análise de qualquer exceção ou caso omisso relacionado à política;
f. Propor ações de segurança da informação alinhadas aos objetivos de negócio do IATec;
g. Registrar, tratar e responder aos incidentes de segurança da informação corporativos;
h. Trabalhar na proposição, construção, análise e manutenção da política e normas de segurança da informação;
i. Propor metodologias de avaliação de risco, que visem minimizar a exposição de dados;
j. Viabilizar a gestão dos riscos de segurança da informação para mantê-los em nível aceitável se apoiando nas informações necessárias para tratamento do risco;

7.7. ENCARREGADO DE DADOS PESSOAIS – DPO

São ações do Encarregado de Dados Pessoais – DPO com apoio e suporte da área de Segurança da Informação:
a. Sensibilizar e informar todos que tratam dados pessoais;
b. Assegurar o cumprimento das Políticas de Privacidade para Colaboradores e Candidatos e Privacidade para Usuários disponibilizadas no site do IATec;
c. Controlar e regular a conformidade das leis de privacidade em vigência;
d. Controlar e acompanhar a produção do RIPD – Relatório de Impacto sobre Proteção de Dados;
e. Promover as abordagens de privacidade por desenho e por padrão (Privacy by design/Privacy by default);
f. Realizar a avaliação na exposição aos riscos de violação de privacidade e mitigá-los aplicando ações de contingenciamento;
g. Manter atualizados os registros das atividades de tratamento de dados;
h. Apoiar os controles de segurança de dados pessoais;
i. Organizar a coleta de informação para identificar atividades de tratamento;
j. Controlar o cumprimento de cláusulas de proteção de dados pessoais junto aos usuários;
k. Ter acesso e autonomia aos fluxos de dados e aos comandos dos controladores para avaliação de conformidade;
l. Realizar contato com autoridades conforme sistema de gestão de segurança da informação.

7.8. DIRETORIA EXECUTIVA

a. Avaliar e aprovar as exceções desta política encaminhadas pelo CSIPD, considerando os riscos originados dessa aprovação;
b. Garantir e prover os recursos necessários para implementar e manter a segurança da informação e os Programas de Conscientização de Segurança da Informação;

7.9. GOVERNANÇA

a. Gerir o processo de mudança do ambiente;
b. Coordenar o processo de homologação de fornecedores observando vigência e finalidade; c. Levantar custos dos serviços suportados pelo IATec;
d. Controlar a estrutura de documentos e procedimentos do IATec.

7.10. SUPORTE & CSM

a. Prover suporte aos produtos do IATec.

7.11. INFRAESTRUTURA

a. Gerir configuração de ativos do IATec;

b. Manutenção da infraestrutura dos ambientes computacionais do IATec;
c. Operar os serviços de infraestrutura garantindo disponibilidade, identificando erros nos ambientes recuperando o serviço, entre outros;
d. Gerir capacidade de infraestrutura;
e. Controlar o acesso ao Datacenter.

7.12. FACILITIES

a. Garantir perímetro de segurança física do prédio, instalações, escritórios e salas do IATec;
b. Controlar acesso físico e monitoramento de ambiente do IATec;
c. Assegurar recursos para a segurança predial.

7.13. GERENCIA DE DESENVOLVIMENTO

a. Promover a adoção de um ciclo de desenvolvimento seguro;
b. Controlar o acesso aos códigos-fonte;
c. Manter um registro das tecnologias utilizadas nos produtos do IATec;
d. Gerenciar a arquitetura dos produtos do IATec e buscar a melhoria contínua;

8. VIOLAÇÕES E OMISSÕES

• Considera-se as seguintes definições:
• Violação: descumprimento, não aplicação ou aplicação incorreta das orientações contidas nessa política de segurança, que afetem a autenticidade, confidencialidade, integridade, disponibilidade e privacidade das informações.
• Omissão: Estar ciente da não conformidade e manter sigilo. Deixar de reportar incidentes ou descumprimento das orientações contidas nessa política de segurança.

9. VIGÊNCIA

Esta Política de Segurança da Informação entra em vigor após sua data de publicação e deve ser revisada anualmente (considerando sua data de publicação ou em caso de alterações significativas).

10. GLOSSÁRIO

Antivírus: aplicação desenhada para proteger o computador de códigos maliciosos.

Backup: Cópia de dados para um local seguro diferente de sua origem, para que possam ser

restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

BYOD: Bring Your Own Device que se encaixam em dispositivos portáreis/móveis ou notebooks particulares.

Confidencialidade: conceito que se aplica a informação que deve ser mantida em sigilo. A informação confidencial deve ser submetida a um conjunto de diretrizes de modo a prevenir o acesso não autorizado.

Controle: qualquer ação, dispositivo, procedimento, técnica ou outras medidas que reduzem exposição ao risco. CSM: Área de aproximação com os clientes visando a melhor experiência ao negócio.

Disponibilidade: propriedade de a informação estar acessível e utilizável quando necessário por entidade autorizada. IATec: Instituto Adventista de Tecnologia.

Incidente de Segurança da Informação: eventos de segurança da informação indesejados ou inesperados com probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação (confidencialidade, disponibilidade e integridade).
Integridade: propriedade de salvaguarda da exatidão e completeza de ativos. A certeza de que uma informação não foi modificada ou alterada de maneira não autorizada.

IoT: qualquer dispositivo computacional que se conecte a rede.

NDA: acordo jurídico de não divulgação.

Norma: conjunto de diretrizes de caráter obrigatório que devem ser operacionalizados para suportar uma diretriz estabelecida na política.

Negócio: unidade/departamento/área específica que cuida de interesses de uma determinada área da instituição considerando a condição do IATec sem fins lucrativos e filantrópicos.

Política: intenção e direção formal e aprovada pela administração da organização.

Propriedade intelectual: visa garantir o direito de domínio e uso de uma criação, assegurando que as vantagens derivadas da exploração de uma criação beneficiem o criador da mesma.

Rede corporativa: grupo de computadores e equipamentos de rede conectados para transmissão e acesso a informações que pertencem ao IATec.

Risco: a probabilidade de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto para a organização.

Software: programa de informática ou aplicação utilizado nos dispositivos eletrônicos.

Squad: Uma squad no desenvolvimento ágil é uma equipe multifuncional, auto-organizada e autônoma que trabalha em conjunto para desenvolver e entregar um produto ou serviço, sendo capaz de tomar decisões relacionadas ao projeto e sendo responsável por todo o ciclo de vida do produto.

Vírus: software malicioso com capacidade para danificar um sistema de computação.

VPN: Virtual Private Network. uma forma de conectar dois computadores utilizando uma infraestrutura de rede pública.

Vulnerabilidade: falha ou fraqueza de procedimento, design, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança.