DOI: 10.22167/2675-6528-20230069
E&S 2023, 4: e20230069
e-ISSN: 2675-6528
REVISTAE&S
Artigo

Gerenciamento de risco para site de instituto de educação

Fabio Luis Gonzaga; Aline Bigaton

Segundo o Project Management Institute (PMI)[1], associação global de gerentes de projetos, risco é todo evento ou condição de incerteza que, quando ocorre, pode causar impactos positivos ou negativos no objetivo do projeto. Os efeitos negativos podem representar ameaças; os positivos, oportunidades. Todos os projetos possuem riscos, e cabe aos membros da equipe de projetos identificá-los para minimizar ou evitar as ameaças e maximizar as oportunidades. O gerenciamento de riscos é um processo que ajuda a identificar, analisar e planejar respostas, além de monitorar esses riscos[2].

Um levantamento realizado pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) mostrou que 54% das empresas brasileiras possuem site, e 57% utilizam a internet como meio para realizar vendas[3]. Empresas cujo site é um componente crítico para o negócio devem gerenciar os riscos relacionados ao custo por tempo de inatividade do site da mesma forma que o fazem para se proteger de perdas como erros, omissões, indenizações trabalhistas, entre outros[4].

A web serve para muitas organizações como parte integrante de suas operações diárias para atrair clientes, comunicar-se com fornecedores e gerar receitas; como resultado, o custo com falhas na disponibilidade de seus serviços pode ser significativo[5]. De acordo com Plesky[6], o tempo de inatividade pode ser definido como o período em que o site está totalmente inacessível ou incapaz de realizar suas funções principais, causando, mesmo que por um período breve, insatisfação aos clientes. Isso pode contribuir para a queda em mecanismos de pesquisa on-line e resultar em perda de clientes e de receita, prejudicando a reputação da marca.

Entre os dias 19 e 23 de fevereiro de 2022, os sites do grupo Americanas S.A., responsável pelos “marketplaces” das Lojas Americanas e do Submarino, apresentaram instabilidades de acesso e ficaram fora do ar, devido a um incidente de segurança. De acordo com a consultoria Economatica, estima-se que a companhia tenha tido um prejuízo de R$ 3,4 bilhões[7] em função do ocorrido.

Os sites podem sofrer com falhas permanentes, intermitentes ou transitórias, afetando a plataforma como um todo ou parcialmente. As falhas permanentes persistem até que o problema seja reparado; as falhas transitórias eventualmente desaparecem sem uma intervenção aparente; e as falhas intermitentes são transitórias e ocorrem ocasionalmente, como, por exemplo, quando há uma sobrecarga no sistema. As causas das falhas podem ser categorizadas como erros de software, de hardware, ambientais ou humanos, além de violações de segurança[5].

Segundo Pertet e Narasimhan[5], a falha se manifesta a partir dos efeitos que são perceptíveis aos usuários; podem-se citar como exemplos exceções do sistema e violações de acesso, que produzem mensagens de erro. Outro tipo de indicação de falha tem ligação com resultados incorretos, a exemplo da exibição de página errada ou em branco ou, ainda, a presença de informações incompletas. Geralmente esse tipo de falha é descoberto somente após as reclamações dos clientes. É possível também ocorrer manifestação de falha de lentidão no desempenho, que pode ser atribuída a vários motivos, entre os quais estão sobrecarga no servidor, travamento de processos, esgotamento de recursos computacionais ou congestionamento de rede.

Dada a relevância do tema, foi realizado um estudo de caso com o objetivo de elaborar um projeto de gerenciamento de risco para o site de um instituto de educação. A pesquisa avaliou como era feito o gerenciamento de risco e qual a percepção dos membros da equipe de

desenvolvimento sobre a importância desse gerenciamento. Depois do diagnóstico, foram listados os principais riscos aos quais os sites estão expostos e, particularmente, o site em estudo. Ao final foi elaborado um plano de respostas aos riscos.

O estudo[8] foi elaborado em um instituto brasileiro de educação e pesquisa, com sede no interior de São Paulo e mais de 500 colaboradores. Entre os serviços oferecidos estavam cursos de graduação e pós-graduação, análises técnicas — principalmente para o setor de agronegócio —, treinamentos de gestão, entre outros. O site escolhido para o estudo fazia parte do portfólio de produtos oferecidos pelo instituto e divulgava em sua página cursos de pós-graduação na modalidade de ensino à distância (EaD).

Esse site foi selecionado como alvo do estudo em função de sua alta demanda de visitantes. Mais de 70% de todo o tráfego era originado de anúncios pagos, o que tornava crítica a necessidade de um site de alta disponibilidade. Ao ser direcionado para a página, o visitante encontrava informações sobre a instituição e sobre cada curso; porém, para se inscrever em um deles, o usuário era direcionado para outro sistema, que coletava dados pessoais e de pagamento.

Uma equipe de desenvolvimento interno era responsável por desenvolver novas funcionalidades, atualizar e manter o site. Esta equipe contava com profissionais de produto, experiência de usuário, designers, desenvolvedores e analistas de dados. A identificação dos riscos foi delimitada ao site objeto de estudo, não estando incluído o sistema responsável por cadastro e pagamento, nem ações de marketing para captação de leads (clientes em potencial). Os riscos levantados referiam-se a falhas que, caso ocorressem, poderiam gerar tempo de inatividade.

A metodologia utilizada na presente pesquisa foi o estudo de caso, que tem como estratégia examinar acontecimentos contemporâneos com técnicas utilizadas em pesquisas históricas, porém acrescentando como fontes de evidência a observação direta e a série sistemática de entrevistas[9].Na primeira etapa mapearam-se as características técnicas do site em estudo, com o propósito de compreender a relação entre o panorama vigente na época e o nível de percepção de risco dos avaliadores no que tangia às ameaças mais comuns em projetos de sites. Para auxiliar no diagnóstico, foi utilizada a lista de riscos comuns do “Project Management Body of Knowledge” (PMBOK)[1], que contém itens, ações e pontos a serem considerados, baseando-se em informações históricas e conhecimento acumulado de projetos semelhantes. A partir do resultado, foram realizadas entrevistas com membros da equipe e com especialistas para a qualificação dos riscos, avaliando as probabilidades e o impacto em caso de ocorrência.

Salles Jr. et al.[8] descrevem que a análise probabilística de eventos geralmente se faz necessária quando faltam informações sobre o processo, o que pode gerar imprecisões. Por isso, quanto mais informações forem obtidas, menos incerto o evento será. Dessa maneira, após a identificação dos riscos comuns do objeto deste estudo, realizou-se uma entrevista, por meio da aplicação de um questionário, com membros da equipe do projeto. O resultado foi um plano de respostas aos riscos, propondo alternativas para prevenir ou reduzir a exposição do negócio a ameaças.

Durante o ciclo de vida de um projeto, os riscos continuam a surgir, e os processos de gerenciamento devem ocorrer de forma interativa; a equipe envolvida no projeto precisa entender se o nível de exposição ao risco é aceitável, e, para isso, devem ser considerados o porte, a complexidade e a importância estratégica do projeto[2].

O site objeto do estudo usava uma plataforma em nuvem especializada na tecnologia e na linguagem de programação para as quais foi desenvolvido. Essa plataforma utilizava variáveis de ambiente de forma segura, evitando que informações sensíveis ficassem expostas no código-fonte ou trafegando por outro meio. Variáveis de ambiente são estruturas importantes com valores dinâmicos que são armazenados de forma temporária no servidor e utilizadas durante a execução de um programa; elas dão suporte para um processo de integração e entrega contínuo, que automatiza e facilita a implantação de novas atualizações e garante que a última versão funcional permaneça disponível caso algum erro seja detectado, diminuindo as chances de uma provável falha no site[10].

Entre os principais recursos oferecidos pela plataforma estavam: suporte à navegação segura por meio do "hypertext transfer protocol secure (HTTPS)" — que funciona como uma proteção para a comunicação e para a transferência de dados entre o navegador web e um site[11] — e do certificado de segurança "secure socket layer (SSL)", um protocolo que exige que o servidor web tenha um certificado digital, funcionando como uma chave pública para transferência de dados por meio dessa conexão[12]. A plataforma oferecia também recursos de mitigação de ataque de negação de serviço distribuído, comumente chamado de ataque "distributed denial-of-service (DDoS)". O ataque de DDoS utiliza milhares de máquinas infectadas para acessar simultaneamente um site, causando uma sobrecarga no sistema e, consequentemente, a negação do serviço por parte do servidor[13].

A atualização do código-fonte era toda feita por meio de processos de versionamento de código, que possibilita obter um histórico confiável das modificações e viabiliza a restauração de uma versão anterior caso um problema ocorra. O acesso ao repositório do código-fonte era restrito aos membros da equipe de desenvolvimento do projeto.

De acordo com Sutherland[14], a definição de feito na metodologia ágil significa que todas as condições e critérios estabelecidos pela equipe foram atendidos, e os testes foram feitos. A equipe do site em questão utilizava como definição de feito para todas as demandas de atualização os seguintes critérios: 1) o incremento deverá passar por testes funcionais, sendo que o testador não deverá ser o mesmo que criou o incremento; 2) o incremento deverá passar por revisão de pelo menos um outro par e ser liberado somente após aprovação; 3) devem ser levados em consideração na criação/desenvolvimento os critérios não funcionais acessibilidade, performance e segurança; 4) deve-se documentar o que foi feito; 5) os critérios de aceite deverão ser atendidos; 6) o incremento deverá estar alinhado às diretrizes de experiência do usuário "user experience" (UX) e "user interface" (UI).

A Tabela 1 apresenta um levantamento de incidentes comuns que podem ocasionar paralisações em sites, baseando-se no histórico de ocorrências reais sofridas em diversas páginas[5],[15]. Existem outros riscos genéricos e comuns que podem causar a indisponibilidade ou afetar a integridade de um site; porém, para este estudo, foram considerados apenas os riscos aos quais acreditava-se que o site estudado poderia estar exposto. Cada risco contém um identificador próprio e a respectiva descrição.

Tabela 1. Riscos identificados

ID	Risco
1	Esgotamento de recursos: vazamento de memória, processos com uso intensivo de recurso, que fazem com que as requisições de páginas atinjam o tempo limite, espaço em disco insuficiente
2	Fatores ambientais: queda de energia, desastres naturais
3	Sobrecarga de tráfego: ocorre principalmente quando há um fluxo anormal de visitantes no site, seja por alguma campanha publicitária, seja por um possível ataque cibernético
4	Tentativas de ataques ou malwares: ataques DDoS, por exemplo, podem levar a uma alta demanda de tráfego no site de forma mal-intencionada, para que ele fique indisponível
5	Erro de codificação: na área da tecnologia, um bug é um erro de codificação em um programa de computador[10]. Infelizmente, nem sempre um bug pode ser detectado de forma rápida

Fonte: Pertet e Narasimhan[5]; Jackson[15]

Durante a análise qualitativa são avaliadas as probabilidades e impactos, o que auxilia a priorização dos riscos. Após identificados os riscos, é possível fazer a qualificação, atribuindo notas para a probabilidade e para o impacto de cada evento[9]. As Tabelas 2 e 3, a seguir, mostram a classificação de probabilidade e o nível de impacto levantados para o site estudado.

Tabela 2. Classificação da probabilidade de ocorrência

Escala probabilística	Grau da probabilidade de ocorrência
0,1	Muito rara a chance de ocorrência
0,3	Baixa chance de ocorrência
0,5	Chance moderada de ocorrência
0,7	Alta chance de ocorrência
0,9	Muito alta a chance de ocorrência

Fonte: Adaptado de Salles Jr. et al.[8]

Tabela 3. Classificação de impacto do evento de risco

Escala probabilística	Grau de impacto
0,1	Muito baixo
0,3	Baixo
0,5	Moderado
0,7	Alto
0,9	Muito alto

Fonte: Adaptado de Salles Jr. et al.[8]

Os impactos foram divididos em três categorias:

- custo: impacto financeiro gerado para a empresa caso o evento de risco ocorresse (por exemplo, a perda de leads se houvesse uma indisponibilidade no serviço que prejudicasse ou impedisse o cadastro);
- estratégico: fato que pudesse impactar o desempenho de uma campanha ou ação de marketing ou prejudicar a imagem da marca;
- qualidade: fato que causasse experiência negativa para o usuário, como lentidão, falha de funcionalidade, problemas de navegação ou página não encontrada.

Após identificados os principais riscos comuns aos quais o site estava exposto, foi realizada uma entrevista por meio de questionário com membros da equipe, com sete respondentes, sendo um gestor de produto e seis desenvolvedores. Cada entrevistado atribuiu um valor aleatório para os riscos identificados, seguindo a escala probabilística de 0,1 a 0,9 para a classificação de probabilidade de ocorrência e nível de impacto do evento de risco, de acordo com as Tabelas 2 e 3, respectivamente.

A Tabela 4 apresenta os riscos priorizados pelo grupo conforme o maior grau de risco calculado (coluna “risco”), o qual foi obtido a partir da multiplicação da probabilidade de ocorrência (coluna “probabilidade”) pelo risco consolidado (coluna “consolidado”), sendo este proveniente do maior valor atribuído como impacto entre as três categorias (custo, estratégico e qualidade).

Tabela 4. Matriz de probabilidade de risco

ID	Evento de risco	Probabilidade	Impacto			Consolidado	Risco
			Custo	Estratégico	Qualidade		
1	Esgotamento de recursos	0,30	0,58	0,72	0,70	0,72	0,21
2	Fatores ambientais	0,21	0,64	0,58	0,64	0,64	0,13
3	Sobrecarga de tráfego	0,50	0,61	0,67	0,67	0,67	0,33
4	Tentativas de ataques ou malwares	0,47	0,67	0,70	0,72	0,72	0,34
5	Erro de codificação	0,55	0,50	0,50	0,55	0,55	0,31
						Risco geral	1,34

Fonte: Adaptado de Salles Jr. et al.[8]

O risco geral do projeto foi normalizado conforme recomendado por Salles Jr. et al.[8], segundo a Equação 1:

$$RGP = \left(\frac{\sum P.I}{n.EP.EI}\right).100 \quad (1)$$

onde, RGP: é o risco geral do projeto; P: são as probabilidades; I: são os impactos; n: é a quantidade de riscos identificados (neste caso, igual a 5); EP: a escala de probabilidades; e EI: a escala de impacto, ambos com valores de 0,9.

Como resultado da normalização no âmbito deste estudo, foi obtido um risco geral de 33%. A percepção de risco elevada se deveu à sensibilidade do projeto, reforçando a relevância do estudo do tema e a necessidade da elaboração de um projeto de gerenciamento de riscos com planos de resposta adequados para cada eventualidade.

O gráfico abaixo, representado pela Figura 1, apresenta a matriz de risco para cada evento de risco identificado. Ela ajuda a entender o grau de percepção sobre a probabilidade de cada evento ocorrer e sobre seu impacto, caso ocorra. A matriz ajuda também a priorizar os riscos de uma forma mais coerente, evitando o uso de suposições.

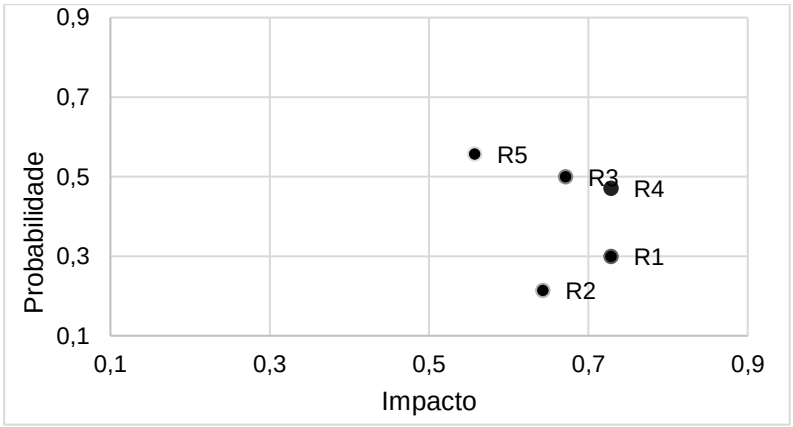

Figura 1. Matriz de risco
Fonte: Adaptado de Salles Jr. et al.[8]

O plano de resposta aos riscos tem como objetivo auxiliar a equipe envolvida no projeto a prever estratégias e ações que devem ser executadas para responder às ameaças identificadas durante o processo de identificação de riscos[8].

Com base na análise de risco feita no estudo, foi elaborado um projeto de gerenciamento de riscos para ajudar na criação de um plano de resposta, com os objetivos de: oferecer diretrizes para a adoção de boas práticas de desenvolvimento e revisão de códigos; descrever possíveis problemas de segurança; orientar quanto ao planejamento do servidor mais apropriado para o site; e recomendar medidas de mitigação de riscos.

Erros ou bugs podem ser causados por ausência ou ineficiência nos processos de revisão de código, falhas ou falta de políticas de segurança para implementação ou ainda pela ausência de boas práticas durante o desenvolvimento. Como resposta, é necessário que a equipe de desenvolvimento implemente processos de revisão de código a cada nova atualização ou manutenção no projeto.

Em uma revisão devem ser observados múltiplos aspectos, como o funcionamento do código, a clareza de sua escrita, a presença de comentários úteis, entre outros fatores. Além disso, o processo de revisão de código pode e deve ser utilizado como parte do processo de melhoria e aprendizagem da equipe de desenvolvimento[16].

É recomendável que a equipe envolvida no projeto continue utilizando o sistema de controle de versão (SCV). A adoção desta prática permite que a cada modificação obtenha-se um histórico de versões anteriores, funcionando como um backup que pode ser restaurado caso haja algum problema em uma nova versão, gerando assim um histórico das mudanças no projeto ao longo de seu ciclo de vida e facilitando o trabalho colaborativo entre os desenvolvedores em um mesmo projeto[17].

Sites estão constantemente suscetíveis a ataques cibernéticos. Entre os principais tipos estão: ataque DDoS; “man-in-the-middle (MitM)”; “phishing”; “spear phishing”; “drive-by”; força bruta; “SQL injection”; “malware”; e “cross-site scripting attack (XSS)”. A Tabela 5 detalha cada tipo de ataque.

Tabela 5. Tipos comuns de ataques cibernéticos em sites

Nome	Descrição
Ataque de força bruta	Neste método de ataque, os hackers utilizam algoritmos que realizam milhares de combinações para descobrir log in e senha
“Drive-by”	Método utilizado para disseminação de “malware”; neste tipo de ataque, os hackers procuram sites inseguros e injetam “scripts” (códigos) maliciosos no protocolo HTTP, por exemplo
“Malware”	Também conhecido como software malicioso, é um programa ou arquivo intencionalmente prejudicial ao dispositivo
“MitM”	Abreviação do inglês para “man-in-the-middle”. Neste tipo de ataque, o invasor se insere entre a comunicação de um cliente e um servidor. São exemplos sequestro de sessão e falsificação de IP
“Phishing” e “spear phishing”	É a modalidade de ataque utilizada para enviar e-mails se passando por fontes confiáveis, com objetivo de obter informações privilegiadas ou influenciar o usuário a realizar alguma ação; outra técnica utilizada pelos golpistas é a clonagem de sites legítimos com a intenção de obter informações pessoais ou credenciais de acesso ao site verdadeiro
“SQL injection”	Termo em inglês para injeção de “structured query language (SQL)”. Linguagem utilizada em banco de dados, é um tipo de

	ataque comum no qual são inseridos comandos SQL, que podem desde capturar, inserir, alterar ou deletar informações de clientes da base de dados
"Cross-site scripting (XSS)"	É um tipo de ataque utilizado principalmente para explorar vulnerabilidades que permitem que, enquanto a vítima navega pelo site, o hacker capture informações armazenadas no navegador, capturas de telas, pressionamento de teclas, informações da rede ou até mesmo controle a máquina da vítima

Fonte: Melnick[13]; Tech Target[11]

Proteger-se desses e de outros ataques requer entendimento do conceito de ofensiva. Para Melnick[13], medidas que visam mitigar as ameaças podem variar, porém existem tratativas básicas sobre como manter sistemas e bancos de dados de vírus atualizados, bom treinamento do time, configuração correta de "firewall", senhas fortes e backups regulares. É importante que o site possua um certificado de segurança, mesmo quando não lide com informações confidenciais. A navegação através do protocolo HTTPS, além de proteger contra o uso indevido do site, é um requisito obrigatório para muitos recursos de tecnologia[18].

Indisponibilidades do servidor podem ocorrer tanto pela ausência de manutenção quanto por defeitos inesperados. É importante a escolha de um serviço de qualidade reconhecida, como a rede de entrega de conteúdo, do inglês "content delivery network (CDN)", que, segundo Plesky[6], pode ser um recurso adotado para criar uma camada entre o servidor em que o site está hospedado e o usuário. O serviço possibilita a entrega de conteúdo por meio de servidores distribuídos geograficamente, utilizando sistemas de cache de conteúdo, o que evita a indisponibilidade do site quando o servidor estiver indisponível por um curto período. O CDN também ajuda a impedir que "bots" (robôs) maliciosos acessem o site, filtrando o tráfego e evitando sobrecarga no servidor.

A plataforma de hospedagem do site estudado oferecia por padrão o serviço de CDN ativo, sem a necessidade de configuração ou contratação adicional. Plesky[6] destaca que a expiração do domínio também pode causar a indisponibilidade do site. O autor recomenda, por isso, a compra por longos períodos ou a renovação automática, caso do domínio do site em estudo.

O tempo de inatividade também pode ser planejado para operações normais de infraestrutura de tecnologia da informação (TI), como backups, atividades de manutenção ou correções de sistema. Porém, a inatividade planejada é um dos principais fatores causadores de incidentes, como, por exemplo, quando um backup demora mais do que o planejado[5].

A plataforma em nuvem do site objeto desta pesquisa tinha "uptime" (tempo em que o servidor está operacionalmente disponível[11]) de 99,99%, garantido pela empresa provedora. A plataforma possuía também uma página para verificação de status dos serviços e canais de suporte para reportar ocorrências de falha.

Foi possível perceber, por meio deste trabalho, que a plataforma estudada tinha um serviço adequado ao porte do projeto; mesmo assim, seria recomendável que avaliasse uma segunda opção de implantação rápida numa hospedagem alternativa, em caso de fatores ambientais que possam indisponibilizar o site por longos períodos. Ter um plano de resposta aos riscos não garante que o site fique completamente seguro, mas ajuda a equipe a pensar proativamente em processos de melhoria contínua.

Como recomendação para complementar este estudo, sugere-se a realização de auditorias periódicas de segurança no site, para encontrar possíveis vulnerabilidades e mitigar a possibilidade de ataques cibernéticos. Concluiu-se que, para o site estudado, a probabilidade de ocorrência dos eventos listados era baixa, principalmente devido às ações de mitigação que já eram adotadas pela equipe de desenvolvimento; os impactos, contudo, podem ser altos caso venham a ocorrer.

Referências

[1] Project Management Institute (PMI). 2021. The standard for project management and a guide to the project management body of knowledge (PMBOK guide). 7ed. Project Management Institute, Newtown Square, PA, EUA.

[2] Project Management Institute (PMI). 2017. Um guia do conhecimento em gerenciamento de projetos. 6ed. Project Management Institute, Newtown Square, PA, EUA.

[3] Empresa Brasil de Comunicação (EBC). 2020. Mais da metade das empresas brasileiras usam internet para vender e 78% estão nas redes sociais. Disponível em: <https://agenciabrasil.ebc.com.br/radioagencia-nacional/acervo/economia/audio/2020-04/mais-da-metade-das-empresas-brasileiras-usam-internet-para-vender-e-78-estao/>. Acesso em: 10 abr. 2022.

[4] Pagely. 2015. Risk Mitigation and the True Cost of Website Downtime. Disponível em: <https://pagely.com/blog/risk-mitigation-and-the-true-cost-of-website-downtime/>. Acesso em: 10 abr. 2022.

[5] Pertet S.; Narasimhan P. 2005. Causes of Failure in Web Applications. Technical Report, Parallel Data Laboratory, Carnegie Mellon University, Pittsburg, PA, EUA.

[6] Plesky E. 2021. What is Website Downtime and Why Should You Take it Seriously? Disponível em: <https://www.plesk.com/blog/various/what-is-website-downtime-and-why-should-you-take-it-seriously/>. Acesso em: 10 abr. 2022.

[7] G1. Tecnologia. Sites de Americanas e Submarino voltam a funcionar após três dias fora do ar. 2022. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/02/23/americanas-tem-site-reestabelecido-depois-de-quatro-dias-fora-do-ar.ghtml>. Acesso em: 10 abr. 2022.

[8] Salles Jr. C.A.C.; Soler A.M.; Valle J.A.S.; Rabechini Jr. R. 2006. Gerenciamento de riscos em projetos. FGV Editora, Rio de Janeiro, RJ, Brasil.

[9] Yin R.K. 2001. Estudo de caso: Planejamento e métodos. 2ed. Bookman, Porto Alegre, RS, Brasil.

[10] Oliveira M.E.; Zuccherelli M.F.L.; Libera G.P.D.; Oliveira R.L.Z.; Tech A.R.B. 2020. Introdução à robótica educacional com Arduíno – hands on!: iniciante. Faculdade de Zootecnia e Engenharia de Alimentos (FZEA/USP), Pirassununga, SP, Brasil. DOI: 10.11606/9786587023052.

[11] Tech Target. 2022. Computer Glossary, Computer Terms - Technology Definitions and Cheat Sheets from WhatIs.com - The Tech Dictionary and IT Encyclopedia. Disponível em: <https://www.techtarget.com/whatis>. Acesso em: 13 set. 2022.

[12] Bhiogade, M.S. 2001. Secure Socket Layer. In: Anais do Computer Science and Information Technology Education Conference; 2002; Cork, Irlanda. p. 85-90. DOI: 10.2139/ssrn.291499.

[13] Melnick J. 2018. Top 10 Most Common Types of Cyber Attacks. Disponível em: <https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/>. Acesso em: 25 jul. 2022.

[14] Sutherland J. 2014. Scrum: a arte de fazer o dobro do trabalho na metade do tempo. LeYa, São Paulo, SP, Brasil.

[15] Jackson B. 2022. Website Downtime: Applicable Tips on How to Prevent It. Disponível em: <https://kinsta.com/blog/website-downtime/>. Acesso em: 24 set. 2022.

[16] Google. [s.d.]. Google Engineering Practices Documentation. Disponível em: <https://google.github.io/eng-practices/>. Acesso em: 28 jul. 2022.

[17] Zolkifli N.N.; Ngah A.; Deraman A. 2018. Version Control System: A Review. Procedia Computer Science 135: 408-415. DOI: 10.1016/j.procs.2018.08.191.

[18] Basques K. 2020. Por que HTTPS é importante. Disponível em: <https://web.dev/why-https-matters/>. Acesso em: 29 jul. 2022.

Como citar

Gonzaga F.L.; Bigaton A. Gerenciamento de risco para site de instituto de educação. Revista E&S. 2023; 4: e20230069.

Sobre os autores

Fabio Luis Gonzaga, Instituto de Pesquisa e Educação Continuada em Economia e Gestão de Empresas – Pecege – Tecnologia da Informação – R. Cezira Giovanoni Moretti, 580 – Santa Rosa – CEP 13414-157 – Piracicaba/SP, Brasil.

Aline Bigaton, Professora orientadora, Pecege - R. Cezira Giovanoni Moretti, 580 – Santa Rosa – CEP 13414-157 – Piracicaba/SP, Brasil.