Segurança da empresa ao software - Será que eu tranquei a porta?

Daniel Paiva Fernandes - Inatel Competence Center
August 16, 2021

Abstract

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

1 Introdução

Não é possível começar o assunto de segurança de informação sem nos inserir no contexto atual. Com efeito da pandemia, muitas empresas se viram obrigadas a se adaptar e alocar seus funcionários, especialmente a força de trabalho ligada direta ou indiretamente como serviços de tecnologia da informação, em regime de trabalho remoto. Esse era um movimento inevitável, não somente no mercado, como em diversos outros setores, e que foi acelerado com a necessidade do isolamento social. Diante disso, surgiram muitas conveniências, mas consigo vieram várias ameaças. Foi criado um cenário ideal para que agentes maliciosos aproveitassem da situação para tirarem proveito de muitos alvos que não estavam preparados para essa migração.

Segundo o IMC Grupo[1], desde que a pandemia começou, o FBI relatou um aumento de 300% nos crimes cibernéticos relatados. Os ataques cibernéticos baseados em nuvem aumentaram 630% entre janeiro e abril de 2020 (Fintech News[2]). E os trabalhadores remotos causaram uma falha de segurança em 20% das organizações conforme levantamento da Malwarebytes [3].

Os prejuízos decorrentes de ataques às empresas tendem à crescer com o tempo. Conforme levantamento da Gartner [4], o mercado de segurança da informação vai atingir o patamar de US$ 170,4 bilhões em 2022, com o investimento das empresas no melhoramento de suas defesas e da ciberresiliência, diante do crescente aumento de ameaças.

Segundo a Accenture[5], o custo médio de um ataque de malware em uma empresa é de US$ 2,6 milhões. Já os os custos de danos do ransomware subirão para US$ 20 bilhões até 2021 e uma empresa será vítima de um ataque de ransomware a cada 11 segundos nesse momento. (Cybersecurity Ventures[6]).

Não é preciso dizer que se a sua empresa ainda não certificou que suas portas estão devidamente trancadas, já passou da hora. Por isso, o nosso objetivo nessa palestra e fazer um apanhado geral de vários pontos que são cruciais para que a sua empresa possa se iniciar, ou amadurecer, os processos relacionados à segurança da informação.

Cada tópico isolado teria conteúdo suficiente para uma apresentação por si. Portanto, apresentaremos os bullet points de cada assunto e faremos uma pequena sessão de hands on para cada ponto em que seja possível fazer uma pequena demonstração.

1.1 Sobre o retorno de investimento

Um estudo publicado pela IBM realizado com 500 empresas pelo mundo, indica que o custo médio por violação dos sistemas informação é de US$ 3,86 milhões. Esse mesmo estudo indica que, uma empresa com automação de segurança totalmente implantada economiza cursos de US$ 3,58 milhões.

Outra informação levantada é que uma empresa que não possui uma equipe preparada para responder aos incidentes de segurança arcam, em média com com US$ 5,29 milhões em custos com violação, na comparação com US$ 2 milhões com empresas que mantêm uma equipe de resposta a incidentes e simulações [7].

Além disso, a credibilidade de qualquer empresa está em jogo com a informações sobre a violação de segurança é divulgada ao público, como o famigerado caso da SolarWinds e, mais recentemente, os ataques de ransonware do grupo REvil sobre várias empresas, como a JBS [8].

1.2 LGPD e GDPR - Fique de olho

Todos já devem estar cansados de ouvir falar sobre a Lei Geral de Proteção de Dados, o Regulamento Geral de Proteção de Dados, entre outras normas com essa finalidade de acordo com a jurisdição que a sua empresa abrange. Mas é importante reforçar, em linhas gerais, alguns aspectos sobre esse assunto antes de adentrarmos na parte prática da apresentação.

A LGPD foi introduzida com a finalidade primordial de regulamentar a conduta das empresas e pessoas físicas para que seja dado o tratamento adequado aos dados pessoais, de forma ética e responsável, focado na privacidade dos dados. A legislação prevê penalizações severas no caso de não-conformidade com as regras ali balizadas.

O mesmo se aplica à GDPR. No primeiro ano em que esse regulamento entrou em vigor, o valor total de multas foi de U$63 milhões [9].

Portanto, um passo muito importante que deve ser considerado durante toda implementação ou amadurecimento de políticas e processos de segurança da informação, deve

levar em consideração não só o conjunto de frameworks e boas práticas, mas também a legislação vigente. Para isso, a melhor recomendação é procurar um profissional especialista em compliance, para auxiliar e avaliar o contexto em que sua empresa se encontra.

2 Por onde começar?

2.1 Qual estado a empresa se encontra?

O processo de gestão e planejamento de segurança da informação é um ciclo contínuo e que depende de constante reavaliação.
Portanto, a primeira etapa para implantar ou reavaliar a situação em que a organização se encontra é analisar o estado em que ela se encontra hoje.
É importante responder as seguintes questões:

1. Qual é o tamanho da organização?
2. Quais os ativos que devem ser protegidos?
3. Quantos projetos existem?
4. Nossos projetos trabalham com informações que extrapolam o campo da segurança e também envolvem a gestão de dados privados?
5. Existe planos de expansão de projetos ou de ativos?
6. Quais são as políticas e estratégias existentes para garantir segurança e privacidade?

A etapa de avaliação do grau de maturidade da organização nesse quesito servirá de patamar para definição de estratégias de implementação e melhoria dos processos relacionados à segurança.
Becker et al. (2009) citado em [10] estabelecem que um modelo de maturidade tem 2 componentes:
i) o meio de medir e descrever o desenvolvimento de um objeto, mostrando a progressão hierárquica;
ii) os critérios para medir os processos
Para isso, existem vários frameworks que trazem modelos de maturidade, como CMMI, C2M2, NIST Cybersecurity Framework.
Citaremos como exemplo aqui CMMI (Capability Maturity Model Integration ou Modelo Integrado de Maturidade em Capacitação), por exemplo, apresenta uma conjunto de níveis de maturidade para melhoria. Na versão 1.3 do CMMI, encontramos as representações contínua ou por estágios.
No modelo de representação contínua, indicado para empresas que desejam focar no amadurecimento de alguns processo, ou se já existe ou modelo contínuo. Aqui, os capacidade de empresa é medida por processos separadamente.
No modelo por estágios, para que o próximo nível de maturidade seja alcançado, todos os processos já devem ter atingido nível anterior.

Figure 1: CMMI v2.0

Já na versão 2.0 do CMMI, temos o modelo de estrutura, divido em 4 categorias, 12 capacidades e 25 áreas de processo.
Com isso, é possível ter uma melhor compreensão do estágio em que a organização se encontra e traçar os próximos artefatos que serão necessários para assegurar a conformidade da empresa com modelos bem definidos de segurança.

2.2 Estabelecimento de Governança e Política de Segurança da Informação baseado nos riscos e ameaças

Incidentes de segurança são os eventos mais temidos por qualquer empresa, gestor ou colaborador. A sua ocorrência pode trazer prejuízos incontáveis, perda de credibilidade da marca ou produto, comprometimento da carreira profissional dos envolvidos, entre outros problemas a se perder de vista.
Se tratando de incidentes, como a organização lida com incidentes no momento?
Para responder esta pergunta, basta analisar casos reais, incidentes registrados pela organização, ou ainda estender o campo de observação para empresas no mesmo ramo de mercado.
No segundo caso, o seu plano de gestão seria capaz de mitigar os incidentes? Em ambos os casos, o que faltou para que o incidente recebesse o devido tratamento?
Para essas e outras perguntas, existem frameworks de gestão de segurança que certamente colaborarão para a implementação de boas práticas que pouparão muita dor de cabeça para sua empresa.
Uma norma bastante popular é a ISO/IEC 27001, per-

tencente ao guarda-chuva da família ISO/IEC 27000. A ISO 27001 traz as diretrizes para gestão da segurança da informação na empresa.

Em seu conteúdo é possível encontrar premissas para adoção de requisitos, políticas, processos, procedimentos, controles e práticas de segurança.

Por sua vez, a norma ISO 27002 traz as boas práticas para apoiar a implementação de um sistema de gestão de segurança da informação (SGSI) como forma de proteger a confidencialidade, integridade e disponibilidade (entre outros requisitos) da informação.

Existem outros frameworks ou normas que podem ser usadas que podem melhor se adequar às necessidades da organização, tais como NIST 800-52, Cobit, ITIL. Ou ainda, a sua empresa pode criar um próprio baseline baseados nos frameworks mencionados.

2.3 Engamento é dever de todos

Durante esse processo de avaliação e implantação, é muito importante não se limitar ao departamento de TI da empresa e, dito isso, estabelecer uma boa relação de confiança mútua com os demais departamentos. Observe a realidade que o cerca em cada um desses ambientes. Quais são os processos, rotinas, fluxos de trabalho.

Uma ferramenta que pode ajudar nesta tarefa é o Microsoft Security Assessment Tdool (MSAT 4.0). É uma ferramente antiga, mas que potencialmente trará insights durante o processo de avaliação de pontos fracos no ambiente de TI.[7]

Apesar de ser uma ferramente antiga, o MSAT é gratuito, e apresenta uma lista priorizada de problemas, ajuda a fornecer orientações específicas para minimizar os riscos mapeados.

Após avaliar o estado de segurança de sua empresa, utilize o MSAT para gerar o PRE e o IDP:

1. *Perfil de risco da empresa (PRE):* Medição dos riscos a que uma organização está exposta, com base no ambiente do negócio e no setor em que ela compete.

2. *Índice de defesa em profundidade (IDP):* Medida das defesas de segurança usadas por pessoas, processos e tecnologias para ajudar a atenuar os riscos identificados para uma empresa.

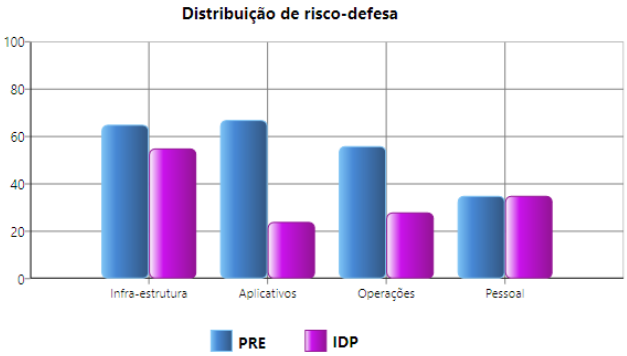

Figure 2: Resultado da avaliação do MSAT 4.0

2.4 Definição de requisitos de segurança

Uma etapa essencial na implementação de segurança da empresa é a definição de um documento de requisitos de segurança, que devem ser baseados em práticas recomendadas pelo setor de atuação, na necessidade do cliente e especialmente nas normas e legislação em que a empresa está sujeita.
O requisito de segurança é uma declaração de funcionalidade de segurança necessária que garante que um das várias propriedades de segurança será satisfeito. Com isso é possível estabelecer um padrão que pode ser reutilizado nos controles de segurança e na adoção de boas práticas.
Por exemplo, a RFC3871 define requisitos de seguranças operacional para infraestrutura de redes de ISP IP networks (roteadores e switches) [11]. Por exemplo:

> 2.2.2. Use Strong Cryptography
>
> Requirement.
>
> If cryptography is used to meet the secure management channel requirements, then the key lengths and algorithms SHOULD be "strong".
>
> Justification.
>
> Short keys and weak algorithms threaten the confidentiality and integrity of communications.
>
> Examples.
>
> The following algorithms satisfy the requirement at the time of writing: AES [FIPS.197], and 3DES [ANSI.X9-52.1998] for applications requiring symmetric encryption; RSA [RFC3447] and Diffie-Hellman [PKCS.3.1993], [RFC2631] for applications requiring key exchange; HMAC [RFC2401] with SHA-1 [RFC3174] for applications requiring message verification.
>
> Para implementar os requisitos de segurança, a OWASP [12] sugere em nível de software, a utilização de quatro etapas:
>
> - Descoberta e Seleção: consiste em compreender os requisitos de segurança de uma fonte e escolher quais deles serão incluídos

no contexto em que se pretende implementar os processos e políticas de segurança

- Investigação e documentação: uma vez selecionados os requisitos, é preciso o verificar cenário atual em face dos novos requisitos de segurança para saber quais requisitos estão sendo cumpridos e quais dependem de alguma implementação.
- Implementação: Naquilo que não se encaixou na etapa anterior, é preciso adaptar à situação para que se satisfaça requisito de segurança e a vulnerabilidade seja mitigada.
- Teste: Depois de tudo, é importante que se elabore casos de teste para confirmar se há ou não alguma vulnerabilidade.

3 Análise de risco e ameaças

A análise de risco é a etapa onde identificamos ameaças potenciais de segurança e privacidade decorrente de vulnerabilidades em produtos, processos e soluções desenvolvidos pela empresa, estimamos os níveis potenciais de risco e propomos ações cabíveis para realizar o tratamento e para mitigar os riscos a um nível aceitável.

3.1 Definição de ativos e classificação de segurança

Os ativos da empresa que nos referimos no contexto da análise de risco, são tudo aquilo que pode estar sujeito a ameaças cuja perda da confidencialidade, integridade ou avaliabilidade podem implicar em prejuízo à empresa.

Podemos citar como exemplo de ativos bens tangíveis, como dispositivos, infraestrutura, e intangíveis como dados, dispositivos lógicos. Alguns exemplos[13] são:

- dispositivos físicos: Roteadores, switches, cabos, servidores, câmeras, equipamentos de laboratório
- software: Sisteas operacionais, firewall, máquinas virtuais
- serviços de rede: VPN, protolocos wireless, redes óticas

3.2 Data flow diagram

O objetivo do Diagrama do Sistema de Informações/Fluxo de Dados é capturar os principais componentes de um Sistema de Informações, como os dados se movem dentro do sistema, pontos de interação do usuário e os limites de confiança.[14]

Um diagrama de fluxo de dados deve[15]:

- Complementar a compreensão da instituição sobre o fluxo de informações dentro e entre segmentos de rede, bem como em todo o perímetro da instituição para partes externas.
- Identifique conjuntos de dados e subconjuntos compartilhados entre sistemas
- Identificar aplicativos compartilhando dados
- Destaque a classificação dos dados que estão sendo transmitidos

Os diagramas de fluxo de dados (DFD) são compostos de formas que criam representações gráficas do seu sistema. Cada forma representa uma função única. Cada interação é analisada para ajudá-lo a identificar ameaças potenciais e maneiras de reduzir o risco.

O uso de formas corretamente permite que você receba melhor contribuição de colegas e equipes de segurança. Todos entenderão como o sistema funciona. Também pode ajudá-los a evitar passar por inúmeros documentos de projeto e planos de desenvolvimento para colocá-los em funcionamento.

- Processo: Representado por um círculo, este elemento representa atividades que podem modificar ou redirecionar a entrada recebida para suas saídas adequadas. Por exemplo, um micro serviço que recebe uma solicitação de chamada de API e encaminha-a para um serviço de manuseio de API; ou um código que valida a entrada de dados antes de ser escrito em um armazenamento de dados
- data store: Representado por linhas paralelas, este elemento representa dados armazenados de forma temporária ou permanente. Como exemplo, é possível citar o uso do cache do navegador para armazenar dados relacionados à sessão do usuário; ou adicionar um evento de registro de segurança a um banco de dados
- Entidade externa: Representada por um quadrado, uma entidade externa pode ser um processo, armazenamento de dados ou até mesmo um sistema completo fora do seu controle direto. Por exemplo, um usuário interagindo com seu serviço, integração com um serviço de autenticação de terceiros
- Fluxo de dados: A movimentação de dados entre os elementos é representada por setas direcionais para indicar comunicação entre a fonte de dados e o destino. Exemplo: quando um usuário envia suas credenciais para acessar um serviço; uma requisição

a partir de um processo para adicionar uma entrada ao seu armazenamento de dados

- Limites de confiança: Representados por linhas pontilhadas ou quadrados, os limites de confiança são usados para descrever o fluxo de dados à medida que cruza diferentes níveis de zona de confiança. Por exemplo: Conexões com serviços de terceiros; ou partes do seu sistema que estão disponíveis somente para administradores

3.3 Classificação de ameaças com STRIDE

STRIDE é modelo de classificação desenvolvido por dois engenheiros da Microsoft no final da década de 1990, e é um acrônimo para seis categorias de ameaças: falsificação de identidade, adulteração de dados, ameaças de repúdio, divulgação de informações, Negação de serviço e Elevação de privilégios.

Especificamente, o STRIDE visa garantir que um aplicativo ou sistema cumpra a tríade da CIA (confidencialidade, integridade e disponibilidade). Seus designers o criaram para garantir que os desenvolvedores de software do Windows considerassem ameaças durante a fase de design.[16]

Cada categoria de ameaça está associada a um controle de segurança (CS) e a elementos do nosso DFD:

Ameaça	CS	DFD
Spoofing	autenticação	Processo, entidade externa
Tampering	integridade	Processo, data store e fluxo de dados
Repudiation	Não-repúdio	Processo, entidade externa e data store
Information disclosure	Confidencialidade	Processo, data store e fluxo de dados
Denial of service	Disponibilidade	Processo, data store e fluxo de dados
Elevation of privilege	Autorização	Processo

Table 1: Relação entre ameaças, controles de segurança e elementos do DFD

- Spoofing: ou falsificação, consiste em passar por alguém.
- Tampering: ou adulteração de dados sem autorização.
- Repudiation: evitar ser responsabilizado por uma ação.
- Information disclosure: acessar dados sem permissão.
- Denial of service: sobrecarregar o sistema para torná-lo indisponível.
- Elevation of privilege: conseguir mais privilégios do que o devido no sistema.

Uma ferramenta útil que pode ajudar a elaborar um DFD é o Microsoft Threat Modeling Tool[17]. Faremos uma rápida demonstração da ferramenta, mas é possível aprender um pouco mais por meio do tutorial disponível em Create a threat model using data-flow diagram elements

3.4 Classificação de dados sensíveis com LINDDUN

Uma forma de classificar ameaças a ativos de privacidade é por meio do LINDDUN, que é uma metodologia que usa uma estratégia um pouco semelhante ao STRIDE, contudo voltado à ameaças contra privacidade. As categorias de ameaças de privacidade são[18]:

- Linkability: ou vinculabilidade, quando um agente malicioso é capaz de vincular dois itens de interesse sem saber a identidade dos dados envolvidos.
- Identifiability: quando um agente malicioso é capaz de identificar um dono de dados a partir de um conjunto de sujeitos de dados através de um item de interesse.
- Non-repudiation: quando o dono de dados é incapaz de negar uma reclamação (por exemplo, tendo realizado uma ação ou enviado uma solicitação).
- Detectability: Um agente malicioso é capaz de distinguir se um item de interesse sobre um dono de dados existe ou não, independentemente de ser capaz de ler o conteúdo em si.
- : Disclosure of information: Um agente malicioso é capaz de aprender o conteúdo de um item de interesse sobre um assunto de dados.
- Unawareness: O dono dos dados desconhece as atividades de coleta, processamento, armazenamento ou compartilhamento (e finalidades correspondentes) dos seus dados pessoais.
- Non-compliance: O processamento, armazenamento ou manuseio de dados pessoais não está em conformidade com a legislação, regulamento e/ou política.

3.5 Identificação e avaliação de riscos e plano de mitigação

Durante a avaliação de riscos, os resultados devem ser documentados e mantidos num plano de tratamento de riscos. A etapa de tratamento de risco consiste em focar sobre os riscos identificados e avaliados, definindo uma prioridade, e onde planejamentos a tomada de decisões sobre como o risco deve ser tratado, como no exemplo da Tabela 2.

Uma forma de classificar os riscos de acordo com a sua natureza no plano de tratamento de riscos pode ser baseado nas seguintes opções de ação[19]:

- Evite - decidir não prosseguir com a atividade que introduziu o risco inaceitável, escolher uma atividade alternativa mais aceitável que atenda aos objetivos do negócio ou escolher uma abordagem ou processo alternativo menos arriscado.
- Reduzir - implementar uma estratégia que seja projetada para reduzir a probabilidade ou consequência do risco a um nível aceitável, onde a eliminação é considerada excessiva em termos de tempo ou despesa.
- Compartilhamento ou Transferência - implementando uma estratégia que compartilhe ou transfira o risco para outra parte ou parte, como terceirizar a gestão de ativos físicos, desenvolver contratos com prestadores de serviços ou garantir o risco. Os terceiros que aceitarem o risco devem estar cientes e concordar em aceitar essa obrigação.
- Aceitar - tomar uma decisão informada de que a classificação de risco está em um nível aceitável ou que o custo do tratamento supera o benefício. Essa opção também pode ser relevante em situações em que um risco residual permanece após outras opções de tratamento terem sido colocadas em prática. Nenhuma outra ação é tomada para tratar o risco, no entanto, o monitoramento contínuo é recomendado.

Event	Action	Plan
Failure to meet compliance obligations	AVOID	Implement formal compliance monitoring process
Loss of Practitioner	REDUCE	Implement succession plan
Failure to collect receivables in a timely manner	REDUCE	Implement receivables tracking and debtor follow-up process:

Table 2: Exemplo de plano de de tratamento de risco[19]

4 Segurança de ativos de informação

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

5 Segurança de pessoas

Com a adoção do trabalho remoto, as informações confidenciais mantidas nas limitações do ambiente de trabalho agora trafegam nas residências de cada colaborador. Com isso, agentes maliciosos passaram a aproveitar da vulnerabilidade de muitas empresas para perpetrar ataques. Segundo o FBI e a Europol, houve aumento nos ataques de engenharia social por meio de phishing, distribuição de malware por anexos maliciosos e ataques de ransonware.

O ativo mais sujeito a vulnerabilidades da segurança da informação é o peopleware. É mais fácil enganar uma pessoa do que encontrar e explorar uma vulnerabilidade no sistema de software, o que leva a crer que as práticas de engenharia social e BEC (business email compromise)

crescerão ainda mais.

O custo por esse tipo de ação maliciosa pode ser irremediável. A empresa Toyota Boshoku Corporation, foi vítima de um ataque de engenharia social e BEC (Business Email Compromise), em 2019, tendo um prejuízo que chega a USD 37 milhões. Pelo mesmo tipo de vetor de ataque, o Condado de Cabarrus, nos Estados Unidos, sofreu prejuízo de USD 1,7 milhão, em 2018[20].

Somado a isso, há a responsabilização das instituições pelo manejo e controle de dados decorrente da LGPD, em vigor, como já mencionado anteriormente. Por estes motivos, a priorização de investimentos em segurança na nuvem e controle de acesso, reforço nas políticas de acesso a dados e informações são prioridade daqui em diante. Além da utilização de ferramentas de reforço à segurança, cabe às instituições fomentar a cultura de conscientização de segurança da informação e o papel que cada colaborador exerce neste ecossistema.

Nem todos colaboradores possuem conhecimento técnico para assumir uma postura consciente de segurança. Até mesmo colaboradores com formação técnica podem ser a causa de vulnerabilidades pelo excesso de confiança.

Programas convencionais de security awareness possuem enfoque na propagação de conhecimento, mas isso não é suficiente para assegurar a mudança de comportamento e adoção de boas práticas. Segundo pesquisa do LastPass em 2017, 59% dos entrevistados compreendiam a importância de senhas seguras e 91% entendiam os riscos de reusar senhas, contudo 41% usavam senhas fáceis de lembrar e 61% usavam senhas iguais ou semelhantes[21].

5.1 Treinamento

Para definir o escopo do treinamento, é recomendado a utilização de survey para coleta de dados quantificáveis e metrificar do estado atual do cenário referente à conscientização, boas práticas e o nível de engajamento dos funcionários da organização, por categoria funcional.

De acordo com o resultado obtido, será possível modelar programas de treinamentos direcionados às áreas mais deficitárias e a papéis exercidos pelos funcionários em suas áreas de atuação.

Possíveis tópicos que poderão ser abordados nos treinamentos incluem:

- Principais vetores de ameaça
  - Identificar Phishing
  - Engenharia social
  - Criação de senhas válidas (utilização de gerenciadores)
  - Cuidados na rede wi-fi doméstica
  - Utilização adequada do equipamento da empresa
- Responsividade a eventos

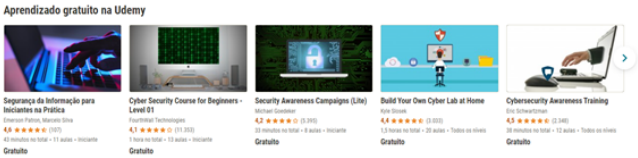

Figure 3: Cursos gratuitos na Udemy

Existem inúmeros cursos gratuitos que podem introduzir os colaboradores nesse processo de conscientização organizacional, em plataformas como o Udemy.

Há ainda outras recomendações, tais como:

- Information Security: Context and Introduction | Coursera
- Cybersecurity for Everyone | Coursera
- NSE Institute: Library (fortinet.com)

Os programas de treinamento podem ser fornecidos aos funcionários em módulos de curta duração e em intervalos moderados, para evitar a saturação de conhecimento.

5.2 Conscientização e avaliação

Poderão ser adotados mecanismos de incentivo e/ou recompensa (gamificação), tais como sistema de pontuação por desempenho nos treinamentos e divulgação de scoreboard, ou criação de programas de recompensa ou vouchers para concessão de descontos em produtos do Inatel ou parceiros.

Neste processo, funcionários que demonstrarem interesse e se destacarem podem servir de embaixadores da segurança

Diante dos resultados, será possível definir novas políticas para reforçar o engajamento dos funcionários no tópico de segurança de informação, por meio de eventos, palestras, summits; simulações com principais vetores de ataque para analisar o resultado dos treinamentos.

Com base nos resultados, será possível realizar novo survey para remodelar o conteúdo do treinamento e progredir no amadurecimento da cultura de segurança da organização, transformando esta etapa num processo cíclico de melhoria contínua.

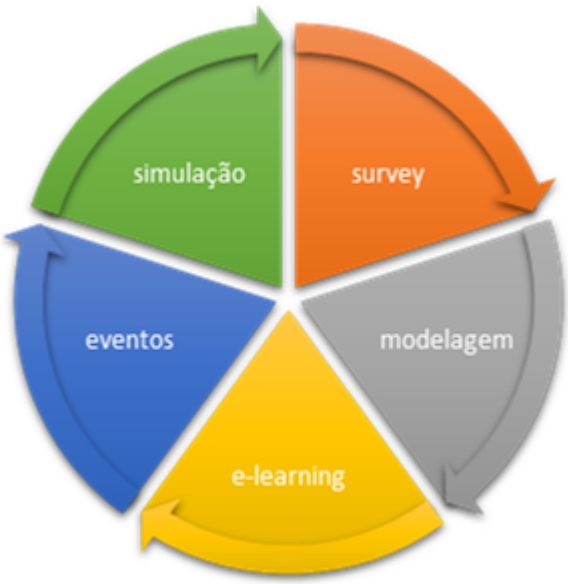

Figure 4: Ciclo de capacitação de pessoal

References

[1] *Covid-19 news: Fbi reports 300 percent increase in reported cybercrimes*, May 2020. [Online]. Available: https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/.

[2] Moccia and P. e. y. n. here, *The 2020 cybersecurity stats you need to know*, Jun. 2021. [Online]. Available: https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/.

[3] *Enduring from home: Covid-19's impact on business security*. [Online]. Available: https://resources.malwarebytes.com/resource/enduring-from-home-covid-19s-impact-on-business-security/.

[4] Gartner$_{I}$nc, *Forecast analysis: Information security, worldwide, 2q18 update*. [Online]. Available: https://www.gartner.com/en/documents/3889055.

[5] K. Bissel, R. M. Lasalle, and P. D. Cin, *Ninth annual cost of cybercrime study*. [Online]. Available: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study.

[6] D. Freeze, *Cybercrime to cost the world 10.5 trillion annually by 2025*, Apr. 2021. [Online]. Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[7] R. S. [mvp], *Microsoft security assessment tool (MSAT) 4.0 and beta 5.0*, Accessed: 2021-6-18, May 2010. [Online]. Available: https://robertsmit.wordpress.com/2010/05/04/microsoft-security-assessment-tool-msat-40-and-beta-50/.

[8] E. Alecrim and M. M. (@Matheus$_{M}$otta), *Jbs pagou us 11 milhões a hackers para evitar vazamento em ataque*, Jun. 2021. [Online]. Available: https://tecnoblog.net/450275/jbs-pagou-resgaste-11-milhoes-dolares-ataque-ransomware-revil/.

[9] *Gdpr fines after one year: Key takeaways for businesses*, Apr. 2019. [Online]. Available: https://gdpr.eu/gdpr-fines-so-far/.

[10] A. J. Azambuja and J. S. Neto, "Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal," *Rev. Serv. Público*, vol. 71, no. 3, pp. 660–712, 2020.

[11] *Rquest for coments: 3871*, Sep. 2004. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc3871.

[12] *C1: Define security requirements*, 2018. [Online]. Available: https://owasp.org/www-project-proactive-controls/v3/en/c1-security-requirements.

[13] *How to complete a clearwater compliance risk analysis information asset inventory*, Mar. 2021. [Online]. Available: https://clearwatercompliance.com/information-asset-inventory-guide/.

[14] *Creating an information system/data flow diagram*. [Online]. Available: https://security.ufl.edu/resources/risk-assessment/creating-an-information-systemdata-flow-diagram/.

[15] *Data flow diagrams 101*, Jul. 2018. [Online]. Available: https://sbscyber.com/resources/data-flow-diagrams-101.

[16] F. Donovan, *What is stride and how does it anticipate cyberattacks?* Jan. 2021. [Online]. Available: https://securityintelligence.com/articles/what-is-stride-threat-modeling-anticipate-cyberattacks/.

[17] *Create a threat model using data-flow diagram elements - learn*. [Online]. Available: https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram-elements/.

[18] [Online]. Available: https://www.linddun.org/linddun.

[19] *Risk management framework - treat risks*. [Online]. Available: https://survey.charteredaccountantsanz.com/risk_management/midsize-firms/treat.aspx.

[20] P. Gatefy, *10 casos reais e famosos de ataques de engenharia social*, Mar. 2021. [Online]. Available: https://gatefy.com/pt-br/blog/casos-reais-de-ataques-de-engenharia-social/.

[21] *New lastpass study finds 92 percent of businesses experience identity challenges*. [Online]. Available: https://www.logmein.com/newsroom/press-release/2019/new-lastpass-study-finds-92-percent-of-businesses-experience-identity-challenges.