FACULDADE DE TECNOLOGIA E INOVAÇÃO – SENAC/DF

GESTÃO DA SEGURANÇA DA INFORMAÇÃO

BRUNO EDUARDO RIBEIRO DA SILVA
LUANA ROCHA ALVES
RAFAEL RODRIGUES LEITE

SGSI

Brasília, DF
2022

RESUMO

O presente trabalho tem como objetivo levantar riscos que possam trazer graves consequências, ocorrendo no presente ou futuro do projeto e-commerce de livraria digital, com a intenção de mitigá-los em sua probabilidade de execução. Dessa maneira, foi feito uma análise minuciosa, de acordo com algumas normas da família ISO 27000 que regem pela segurança da informação para serem implementadas. Além disso, todas as políticas adotadas serão de acordo com a Lei Geral de Proteção de Dados, trazendo penalidades caso não cumpridas dentro desse Sistema de gerenciamento de segurança da informação apresentado.

Palavras-chave: Risco. Análise. ISO 27000. Segurança da Informação. Políticas. Lei Geral de proteção de dados. Sistema de gerenciamento de segurança da informação.

SUMÁRIO

1 INTRODUÇÃO

Nosso projeto trata de uma livraria digital que vende livros físicos de vários tipos, voltados tanto para a parte didática como recreativa.

O projeto abrange as unidades físicas de armazenamento do material, contando com vários armazéns espalhados por Brasília. A parte lógica delimita o uso do site da loja e o aplicativo mobile para praticidade de uso. Nosso escopo aborda a proteção do patrimônio físico da empresa como os depósitos e o conteúdo impresso, bem como a parte lógica com a gestão dos dados dos clientes tais como logins, meios de pagamento e carrinho de compras.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Compreender o Sistema de Gerenciamento de Sistemas de Informação criado em viés da livraria digital, visando incluí-la dentro dos quatros atributos que regem um SGSI. São eles: Estabelecer, implementar, monitorar e manter.Dessa forma, o presente projeto propõe concatenar todos os quesitos necessários para montar esse sistema.

2.2 OBJETIVOS ESPECÍFICOS

Identificar, prevenir e tratar riscos lógicos;
Gerenciar riscos do ambiente físico da empresa;
Auditar e monitorar as atividades realizadas pela empresa;
Analisar potenciais riscos a empresa;
Planejar uma rotina de contingência para eventuais incidentes; e
Implementar e gerir a aderência da ISO 27000.

3 PLANEJAMENTO ESTRATÉGICO DA SEGURANÇA DA INFORMAÇÃO

-Missão: Prover soluções de riscos para a segurança da informação nos processos da livraria digital.

-Visão: Ser referência pelo cumprimento do Sistema de Gerenciamento de Segurança da informação implementado no *e-commerce*

-Valores: Inovação, qualidade, Segurança, transparência e eficiência.

Π

4 ANÁLISE DE RISCO E PLANO DE CONTINGÊNCIA

De acordo com a NBR ISO IEC 27005/2019 (Cap 8.2) é necessário identificar os riscos que ocorrem ou que podem vir a ocorrer, para que dessa forma identifique sua probabilidade e impacto na segurança da informação da organização, assim fazendo sua análise de riscos. Dessa maneira, por meio da técnica checklist foram identificados os riscos que podem afetar o desenvolvimento deste e-commerce com nicho de venda de livros. São eles:

-*Chargeback;*
-Problemas nos CMS(Sistema de gerenciamento de conteúdo);
-Disponibilidade de estoque;
-Segurança do servidor em nuvem;
-Controle de acessos;
-Atualização de Software; e
-*Pharming.*

Em virtude desses riscos identificados, podemos levantar as consequências que acarretam, caso sendo expostos a tais vulnerabilidades, observando-se suas ameaças ao realizar tais feitos:

Riscos	**Vulnerabilidades**	**Ameaças**	**Consequências**
Chargeback	Não ter controle de permissões de identificação de transações suspeitas	Usar conta bancária do titular para fraudar na compra.	Perda de retorno financeiro na venda dos livros.
Problemas nos CMS	Não atualizar conteúdo exposto na plataforma, sem a segurança do código do desenvolvimento.	Compras realizadas abaixo do valor atual do produto.	Perda de controle de preços e valores aos quais os livros foram vendidos.
Disponibilidade de estoque.	Não manter o controle da logística atualizado juntamente com o site.	Compra de um produto que não está disponível.	Perda de controle de envio de produtos a serem enviados aos clientes.

Segurança do servidor em Nuvem	Não a configurar da maneira correta.	Ataques de hackers com má intenção.	Perda da credibilidade da segurança dos dados.
Sem controle de acessos	Deixar acessos dentro da organização abertos para todos os funcionários.	Modificar, configurações de setores responsáveis.	Perda de controle de quem acessa ou interferir em algo, assim tendo algum erro, não sabendo identificar o responsável.
Atualização de Softwares	Abster-se de novas versões de sistemas ou melhores sistemas.	Sujeita a ataques de cibercriminosos	A organização fica defasada no mercado.
Pharming	Não escolher um provedor de internet confiável.	Ataque ao DNS do e-commerce.	Falta de credibilidade dos clientes sobre a segurança de seus dados

Dessa maneira, após riscos levantados, iremos fazer uma análise qualitativa para entender: Qual a probabilidade desse risco acontecer? E caso ocorra, qual nível o impacto acarretará?

Sendo assim, medindo e comparando os riscos, a equipe precisará mitigar e dar prioridade a eles, dependendo de seu nível de sua probabilidade e impacto de acordo a análise preliminar de risco (APR) abaixo:

Risco	**Probabilidade**	**Impacto**	**Classificação**
Chargeback	M	A	Alto
Problemas nos CMS	A	A	Alto
Disponibilidade de estoque.	M	A	Alto

Segurança do servidor em Nuvem	A	A	Alto
Sem controle de acessos	B	A	Médio
Atualização de Softwares	B	M	Baixo
Pharming	M	A	Alto

		IMPACTO		
		B	M	A
PROBABILIDADE	A			2
	M			3
	B		1	1

Baixo(B)

Médio

Alto

O plano de contingência ou plano de tratamento de riscos, como colocado na ISO 27005, tem como objetivo planejar uma ação caso os riscos levantados ocorram, ou seja, seria se precaver. Nesse sentido, ela forma um plano de ação, caso ocorra por meio de planos estabelecidos, sob responsáveis e como iram tratá-los diante destes cenários:

Situação de Risco	**Quando fazer?**	**Gatilho**	**Responsabilidade chave**	**O que fazer?**
Chargeback	Solicitação do cliente para devolução de produto por não reconhecimento de compra	Aviso de pedido demasiado de estorno	Equipe Jurídica	Entrar em contato com a vítima e entender os fatos para prestar apoio e adotar políticas de segurança
Problemas nos CMS	Quando o conteúdo não estiver atualizado	Aviso de falta de insights no site	Marketing	Atualizar de imediato o conteúdo a ser posto na livraria
Disponibilidade de estoque	Falta de produto no estoque	Aviso de alta demanda e falta de produto	Logística	Identificar mercadoria com escassez e solicitar
Segurança do servidor em Nuvem	Algum alarme de ataque iminente.	Aviso de alerta do servidor	Especialista de computação em nuvem	Utilizar ferramentas definidas para atuarem contra invasão
Sem controle de acessos	Quando não ocorrer solicitação de acessos.	Aviso de acessos indevido de um indivíduo	TI/ Gestores de departamento	Restringir acesso e distribuir conforme as responsabilidades e termos de políticas internas.
Atualização de Softwares	Quando já não acompanha o mercado	Bugs causados por desatualização	Equipe de TI	Solicitar a disponibilização dos softwares e treinamento .

Pharming	Modificação das DNS redes de computadores	Aviso de réplica de sites falsos	TI/ Redes	Identificar réplica e derrubar sua DNS atrelada ao site original.

5 ISO 27000

A série de normas da família ISO, tem como função delimitar regras de conduta para melhor gestão técnica de um empreendimento. Por se tratar de uma família a ISO aborda vários modelos de negócio e tem suas próprias características para cada um deles abordando boas práticas em gestão, segurança e governança. Podemos citar as ISO 270001, 27002, 27003, 27004, 27005 e 27006.

Cada uma delas tem suas próprias diretrizes e o seu escopo varia bastante de acordo com o objetivo específico. Neste documento abordamos brevemente alguns dos tópicos das ISO 27001, 27002, bem como a 27005.

6 SEGURANÇA FÍSICA

A segurança física da empresa irá abranger protocolos de segurança a serem adotados para as instalações físicas do e-commerce, mais especificamente no que tange a gestão dos diversos armazéns espalhados por Brasília-DF nos quais são armazenados os produtos físicos comercializados através da loja.

A ISO 27002 versa sobre os parâmetros ideais para segurança física e do ambiente. No caso do nosso *e-commerce* a segurança física não irá englobar grandes servidores para processamento de dados uma vez que serão utilizados os serviços em nuvem oferecidos pela Amazon Web Services (AWS). Tal serviço foi escolhido devido à escalabilidade inerente à modalidade de computação em nuvem que permite a ampliação ilimitada do armazenamento de toda a infraestrutura, softwares e servidores da empresa, facilitando assim futuras expansões da loja.

Assim, a segurança física da empresa irá abordar as melhores práticas previstas na ISO 27002 para a proteção dos ativos mais sensíveis à loja: seu estoque de livros físicos e os armazéns que os estocarão.

Em relação às áreas seguras dos armazéns estes deverão possuir:

Perímetro de segurança física

- Perímetro devidamente delimitado com grandes cercas e arames farpados, de maneira a evitar o acesso indevido às instalações.
- Grande número de câmeras de vigilância com sensor de movimento que, no período com menor incidência de luz, ativem grandes refletores.
- Paredes, janelas e portas robustas e com alarmes sonoros em caso de violação que já acionem as forças policiais automaticamente.
- Sensores e alarmes de incêndio, bem como extintores, sistemas de alta pressão com mangueiras e esguichos.
- Para-raios espalhados pelo complexo com o devido aterramento.
- Colaboradores exclusivos para a segurança do espaço físico.

- Guaritas separadas, ambas com cancelas reforçadas, sendo que uma controla o acesso dos colaboradores da empresa ao espaço interno e outra controlando o acesso dos caminhões de entrega às docas de despacho das mercadorias (livros).

Controles de entrada física

- Controle de acesso de ao espaço interno do armazém a ser realizado nas guaritas, no qual deverá constar identificação do veículo, bem como a de seus ocupantes
- Controle de acesso dos colaboradores através de crachás de identificação e ponto eletrônico obrigatório na entrada e saída destes.
- Controle de acesso à área exclusiva do estoque, somente colaboradores com a devida autorização podem acessar tal área ao submeter sua digital à trava biométrica.
- Fornecedores, partes externas (suporte) e todos os visitantes deverão obrigatoriamente portar adesivos os identificando e não devem transitar sem o devido acompanhamento de colaboradores da empresa.
- Os direitos de acesso às áreas seguras dos armazéns serão revistos e atualizados em intervalos regulares, podendo ser revogados quando necessário.

Áreas de entrega e de carregamento

- As docas de entrega e carregamento estão localizadas nos fundos dos armazéns (sem conexão com outras partes dos edifícios) e possuem guarita individual para o controle de acesso, garantindo que os entregadores não tenham acesso a outras partes dos armazéns.
- Os materiais entregues serão inspecionados e examinados para a detecção de qualquer ativo nocivo antes de serem devidamente armazenados.
- Separação das remessas entregues das que saem, bem como o devido registro para o gerenciamento de estoque.

Equipamentos

- Todos os computadores e ativos eletrônicos devem estar em locais monitorados e devidamente instalados para minimizar o risco de ameaças físicas potenciais.
- Não é permitido o consumo de alimentos, bebidas ou fumar na área de trabalho com computadores, para isso os colaboradores deverão utilizar a copa, bem como do espaço externo reservado para tais atividades.
- Instalações elétricas robustas e completamente aterradas seguindo as melhores práticas de qualidade.

Segurança do cabeamento

- Todas as linhas de energia e de telecomunicação que adentram os armazéns deverão ser subterrâneas.
- Os cabos de energia devem obrigatoriamente estar separados dos cabos destinados às telecomunicações, evitando assim interferências eletromagnéticas.
- O acesso aos painéis de conexões e saídas de cabos será sempre controlado e supervisionado.

Manutenção dos equipamentos

- A manutenção de todos os ativos físicos deverá ser realizada nos intervalos recomendados pelo fornecedor e de acordo com suas especificações.
- Somente pessoal de manutenção autorizado devem proceder com a manutenção e consertos dos ativos.
- O setor responsável pelo patrimônio da empresa é responsável por catalogar todos os ativos, bem como os registros de todas as manutenções preventivas e corretivas já realizadas, além das futuras.

Armazenamento dos Livros

- Os livros deverão ser armazenados em caixas e em prateleiras robustas que comportem seu peso, bem como possuir temperatura

ambiente e umidade controladas, seguindo as orientações oferecidas pelas editoras para a preservação do acervo.

- Deverão estar dispostos seguindo o padrão organizacional adotado pela empresa, facilitando a localização de cada livro no estoque e permitindo rápida reposição quanto separação para envio.

Equipamento de usuário sem monitoração

- Todos os colaboradores com acesso a computadores pessoais nos ambientes dos armazéns deverão proteger tais equipamentos quando estes estejam desacompanhados.
- Os colaboradores devem encerrar as sessões ativas ou bloquear o acesso através de senha quando se ausentarem de suas máquinas, bem como encerrar aplicativos sensíveis à empresa quando não estiverem em uso.

Política de mesa limpa e tela limpa

- Qualquer informação sensível ou crítica envolvendo os negócios da empresa, estando em papel ou em mídia de armazenamento eletrônicas devem ser armazenadas em arquivos protegidos ou gavetas chaveadas quando não estiverem em uso.
- Todos os computadores quando não estiverem em uso devem ser mantidos desligados e possuir bloqueio e acesso mediante senha e identificação pessoal do colaborador.
- Documentos com informações sensíveis devem ser removidos das impressoras assim que sejam impressos.

7 SEGURANÇA LÓGICA

A parte de segurança lógica da empresa prevê que tanto o site quanto o aplicativo móvel da loja devem ter protocolos de segurança para proteger os dados dos clientes e da empresa como um todo.

Temos ciência de que informações de login, carrinho de compras, meios de pagamento são apenas alguns dos aspectos técnicos a serem levados em consideração quanto aos riscos e as necessidades de confiabilidade, disponibilidade e confidencialidade. Por operar de maneira 100% digital, a loja tem que tratar dados como inventário, estoque, preços e entregas de maneira automatizada e segura. Quanto às tecnologias utilizadas para realização dos serviços principais, o servidor proxy utilizado pela empresa irá gerir o tráfego de rede e garantir que os clientes tenham acesso aos produtos e ao site de maneira integral visando a maior disponibilidade e segurança.

Um roteador com filtro de pacotes é utilizado para garantir que o tráfego indevido de pacotes com conteúdo malicioso chegue aos computadores da empresa. O firewall de maneira semelhante filtra o tráfego da rede e possíveis ameaças impedindo que cheguem às máquinas ou de se propagarem pela rede. A criptografia permite que senhas e logins de usuário, assim como informações financeiras e endereços sejam armazenados e tratados de maneira segura permitindo que apenas o banco de dados possa comparar o código *hash* dos dados inseridos com o que foi disponibilizado pelo usuário previamente no cadastro.

Por último mas não menos importante o antivírus permite diagnosticar e prevenir vírus em máquinas chaves do sistema, em último caso o deve-se eliminar o vírus e checar a integridade dos dados que possam ter sido afetados pelo malware.

A ISO 27005 prevê que a identificação das vulnerabilidades é parte crucial do tratamento dos riscos e pode ajudar a mitigar os impactos negativos de uma situação, seja ela um vazamento, ataque direto ou problemas internos em geral. Como abordado na ISO 27001, um dos meios de proteção de ativos consiste no backup recorrente das informações para gerar redundância e garantir que em casos

de modificação indevida ou perda de dados exista um repositório capaz de suprir as necessidades da empresa.

Outro tópico delimita que a aquisição, desenvolvimento e manutenção dos sistemas pressupõe que a nossa empresa irá adquirir serviço de hospedagem de site e aplicações voltadas para a nuvem para facilitar a gestão e manutenção deles. Os dados financeiros devem ser tratados de maneira sigilosa e assim como os dados do cliente e dos softwares usados.

A gestão de incidentes deve assegurar que possíveis eventos contra a empresa sejam identificados em tempo hábil para sua correção e tratamento assim como disposto na ISO 27002.

O engajamento de nossos funcionários é parte importante de nossas políticas, de maneira que o ambiente deve proporcionar uma escalabilidade dos protocolos de segurança. Com a atualização de nossas políticas e o desenvolvimento delas, nossos colaboradores devem adotar políticas de boas práticas (Como abordado na ISO 27002) e se manterem a par dos novos riscos presentes em seu meio de atuação.

8 FERRAMENTAS

\

Amazon EC2 (Computação em nuvem)

Amazon Dynamo (Banco de Dados)

Amazon SNS (Front-end)

Amazon GuardDuty (Segurança)

AWS Network Firewall (Firewall)

Norton (Antivírus)

PagSeguro (Sistema de pagamento)

Zoho Inventory (Sistema de gestão de estoque)

9 LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

A LGPD impõe o dever de proteção de dados pessoais tanto às pessoas físicas quanto jurídicas.

Para o total cumprimento das disposições contidas na Lei Geral de Proteção de Dados Pessoais (13.709/2018), todos os dados pessoais que estejam sob posse desta empresa serão organizados e categorizados possibilitando rápido acesso a todas as informações, sendo que as mais sensíveis receberão tratamento mais rigoroso.

Todos os dados pessoais também devem ter seu fluxo monitorado, através de softwares de cibersegurança que gerem relatórios periódicos que auxiliarão as auditorias impostas pela referida Lei.

A empresa deve implementar um programa de governança de dados que deverá: categorizar e classificar os dados armazenados, bem como determinar quem pode ter acesso a eles e quem será responsável por monitorar todo esse processo.

Em atenção ao disposto no capítulo VI, seção II, art. 41 da Lei, a empresa deverá indicar o colaborador denominado DPO, encarregado pelo tratamento de dados pessoais. Ele será o responsável por cuidar dos dados, bem como prestar esclarecimentos.

10 VIOLAÇÃO DAS POLÍTICAS DA SGSI

Qualquer violação de segurança deve ser informada à área de Segurança da Informação para a devida investigação e determinação das medidas necessárias para a correção da falha ou reestruturação de processos.

São consideradas violações de segurança:

- Uso ilegal de Software;
- Introdução (intencional ou não) de vírus;
- Compartilhamento de dados sensíveis da empresa;
- Divulgação de informações pessoais de clientes e das operações contratadas;

Importante ressaltar que os princípios de segurança estabelecidos no presente documento possuem total aderência da presidência e diretoria da empresa e devem ser observados por todos os colaboradores no desempenho de suas funções.

As penalidades pelo descumprimento das políticas e diretrizes aqui dispostas estão previstas no contrato de admissão de funcionário.