UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

AUGUSTO LEITE SANTOS SUBA

METODOLOGIA PARA INSTITUCIONALIZAÇÃO DE NORMAS DE SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE CORPORATIVO

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2020

AUGUSTO LEITE SANTOS SUBA

METODOLOGIA PARA INSTITUCIONALIZAÇÃO DE NORMAS DE SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE CORPORATIVO

Trabalho de Conclusão de Curso de Graduação, apresentado ao Curso Superior de Tecnologia em Sistemas de Telecomunicações, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. Christian C. S. Mendes

CURITIBA
2020

TERMO DE APROVAÇÃO

AUGUSTO LEITE SANTOS SUBA

METODOLOGIA PARA INSTITUCIONALIZAÇÃO DE NORMAS DE SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE CORPORATIVO

Este trabalho de conclusão de curso foi apresentado no dia12 de novembro de 2020, como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. O aluno foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Daniel Fernando Pigatto
Coordenador de Curso
Departamento Acadêmico de Eletrônica

_____
Prof. M.Sc. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

_____
Prof. Dr. Daniel Fernando Pigatto
UTFPR

_____
Prof. Dr. Luiz Carlos Vieira
UTFPR

_____
Prof. Christian C. S. Mendes
Orientador - UTFPR

“A Folha de Aprovação assinada encontra-se na Coordenação do Curso”

À minha esposa, exemplo de dedicação e estudo, que me ajudou nas horas mais difíceis, e incentivou durante todo o trajeto. Ao meu filho que mesmo na minha ausência conseguiu compreender a importância de tudo o que fiz.

AGRADECIMENTOS

A Deus, que me deu forças por estes dois últimos anos em momentos que mais precisei.

Ao corpo docente desta instituição, que vai além de nos apresentar aos conhecimentos técnicos relativos ao curso, nos mostrando o amor deles pela posição de ensinar, e nos fazendo sentir esse intenso amor pela instituição, nos dando mais formação de base profissional e pessoal.

À família, que sem ela não teria caminhado com os passos certeiros e seguros, e que sempre que eu cai foram os responsáveis por me ajudar a levantar.

Aos amigos que fiz durante todo este processo, e que com certeza ficaram guardados nossos momentos de aprendizado.

A todos que de alguma forma fizeram parte desta etapa de minha vida, me incentivando, me orientando ou me corrigindo, o meu muito obrigado.

RESUMO

SUBA, Augusto L. S. **Metodologia para Institucionalização de Normas de Segurança da Informação em um Ambiente Corporativo**. 2020. 65 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020.

Este trabalho tem como objetivo desenvolver uma nova política de segurança da informação, para uma empresa privada com base nas normas da ABNT e nas leis atuais vigentes. Para isso foi usado como base a política atual da empresa, e realizadas pesquisas de boas práticas de segurança da informação atuais bem como os ajustes necessários para o enquadramento da política a nova Lei federal de proteção de dados pessoais. Como resultado, foi gerada uma nova política atualizando os padrões de segurança da empresa e ofertando diretrizes para a melhoria contínua daqui em diante.

Palavras chave: Segurança da Informação. Política de Segurança. Normas.

ABSTRACT

SUBA, Augusto L. S. **Metodologia para Institucionalização de Normas de Segurança da Informação em um Ambiente Corporativo**. 2020. 65 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020.

This work aims to develop a new information security policy for a private company based on ABNT rules and current laws. For this purpose, the company's current policy was used as a basis, and research on current good information security practices was carried out, as well as the necessary adjustments to fit the policy to the new federal law on the protection of personal data. As a result, a new policy was created updating the company's safety standards and offering guidelines for continuous improvement from now on.

Keywords: Information security. Security policy. Standards**.**

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

ABNT	Associação Brasileira de Normas Técnicas
B2B	*Business to business*
B2C	*Business to consumer*
ISO	*International Organization for Standardization*
ITS-RIO	Instituto de Tecnologia e Sociedade do Rio de Janeiro
SUS	Sistema Único de Saúde
SGSI	Sistema de Gestão da Segurança da Informação
LGPD	Lei Geral de Proteção de Dados
PSI	Política de Segurança da Informação
DP	Dados Pessoais
SGPI	Sistema de Gestão da Privacidade da Informação

SUMÁRIO

1. INTRODUÇÃO

Historicamente, a informação auxilia a sociedade no seu processo de evolução através da comunicação, que transmite a informação de um indivíduo para o outro, tornando a informação um ativo capaz de transformar crenças, valores e comportamentos (COSTA, 2014).

No meio corporativo, a informação é um dos bens mais valiosos, possuindo esse agente transformador que pode alavancar uma instituição - quando bem gerenciado, servindo como base para diversas ações de tomada de decisão, planejamento e estratégias (LOUSADA e VALENTIM,2010).

A segurança da informação cada vez mais é observada e aplicada, pois as empresas passaram a atentar-se ao fato de que essas medidas podem representar ganhos financeiros e competitivos em relação ao mercado.

Há diversos casos de roubos de informações que ficaram conhecidos na mídia devido ao impacto causado em empresas “alvo”. Um exemplo é o caso da Aadhaar Services que teve suas informações roubadas e vendidas via WhatsApp pelos contraventores entre novembro de 2017 e janeiro de 2018 (KHAIRA, 2018). O material continha dados pessoais dos cidadãos indianos e fazia parte de um processo de unificação de sistemas, que visava garantir à população acesso a serviços governamentais básicos. Entre os dados vazados estavam os telefones e endereços de todo cidadão que já havia passado pelo processo.

Em 2016 a Uber, empresa multinacional americana prestadora de serviços eletrônicos na área de transportes privado urbano, teve os dados de cerca de 57 milhões de usuários e motoristas roubados por *hackers* (EFE, 2017). Além do número de clientes/colaboradores afetados um dos pontos que chama a atenção neste caso, foi a forma como a empresa tentou esconder a notícia inclusive pagando cerca de U$ 100 mil aos *hackers* responsáveis pela violação, solicitando a destruição da informação roubada, que continham dados como: nomes, e-mails, telefones e números de documentos dos motoristas.

A empresa espanhola Prosegur tem seu foco em segurança privada, teve sua rede invadida por um vírus *trojan* que criptografou arquivos do sistema (WAKKA, 2019). Em novembro de 2019 a empresa adotou medidas de segurança, enviando

seus colaboradores para casa e os sistemas da empresa ficaram cerca de 24 horas fora do ar.

Estes fatos não são isolados e a cada ano que passa vemos esses incidentes se repetirem em diversas empresas no mundo, contudo existem maneiras de se reduzir o impacto ou até mesmo proteger totalmente a informação de uma empresa, seguindo algumas diretrizes criadas por organizações focadas em normas e padronizações, e que auxiliam às empresas a proteger suas informações.

Essas normas oferecem métodos e processos desenvolvidos e aplicados mundialmente, que aumentam a segurança das informações através de boas práticas, rastreio e processos de segurança digitais e físicos, oferecendo a empresa um ambiente mais seguro e dentro das leis locais.

No Brasil, desde 1940, existe uma entidade reconhecida pelo governo federal brasileiro: a Associação Brasileira de Normas Técnicas – ABNT. Além da criação de normas, a ABNT ajuda a promover o desenvolvimento do mercado brasileiro, bem como contribui para a implementação de políticas públicas, visando a segurança dos consumidores e cidadãos.

Em 1946 na Inglaterra (ISO, 2019) a ABNT foi umas das entidades presentes durante uma conferência realizada para a criação da padronização internacional, e assim em 1947 surgia a *International Organization for Standardization* – ISO. A ISO surgiu com 67 delegados *experts* em assuntos específicos, com a missão de auxiliar o desenvolvimento de mercados internacionais através da criação de normas documentadas para auxiliar as empresas com diretrizes globais para produção e processos.

Tendo em vista os fatos relatados, no que se refere a segurança, pode-se observar que todas as empresas podem ser alvo de fraudes e falhas na segurança das informações. Por outro lado, vemos que as entidades normativas trazem processos e apresentam métodos cada vez mais elaborados para a proteção dessas informações, auxiliadas pelas evoluções tecnológicas.

Este trabalho apresentará uma nova política de segurança da informação, considerando as leis e normas atuais, melhorando consistentemente à política de segurança da informação existente de uma grande empresa.

1.1 PROBLEMA DE PESQUISA

A constante evolução tecnológica e normativa pode tanto dificultar como auxiliar na proteção de informações, observando que ao mesmo tempo que os contraventores dispõem de mais ferramentas para a captura dessas informações ao mesmo tempo que as equipes de segurança da informação descobrem novas formas de defende-las.

Tendo por base que a política de segurança de informação criada há 5 anos que tende a estar desatualizada, este trabalho propõem uma nova política de segurança que esteja de acordo com essas atualizações e as leis vigentes.

1.2 DELIMITAÇÃO DO PROBLEMA

O objeto de estudo deste trabalho é a política de segurança da informação de uma grande empresa do ramo de filantropia, aqui denominada “Grupo X” e com sede em Curitiba, PR.

O Grupo X possui atuação nas áreas de saúde (administração de hospitais) e educação (administração de Universidades e Escolas do ensino fundamental ao médio), tendo assim uma grande diversificação de clientes, ao mesmo tempo que necessita armazenar, gerir e proteger uma variedade imensa de informações.

1.3 JUSTIFICATIVA

A proteção das informações de uma empresa, possibilita uma maior competitividade e garante que as estratégias de alocação de recursos, e/ou investimentos, sejam reveladas apenas nos momentos propícios à sua apresentação.

Deve existir também o cuidado com a informação de terceiros (funcionários, clientes e fornecedores), que é abordada de forma mais específica pela Lei Geral de Proteção de Dados de 2018 (LGPD), responsabilizando a empresa por toda informação que possui sob sua guarda, podendo implicar em sanções no caso de extravio, vazamento e outras situações que possam vir a gerar ônus ao terceiro ao qual a informação se refere (LEI Nº 13.709,2018).

A criação de uma política de segurança da informação (PSI) não garante a proteção da informação, dependendo essencialmente da boa execução prática de suas diretrizes e um bom alinhamento dos processos executados com a PSI,

necessitando assim, do envolvimento da diretoria para outorgar a implementação e divulgar amplamente a relevância do assunto.

Este trabalho apresentará a proposta de uma nova política de segurança da informação, corrigindo as possíveis falhas e atualizando-a de acordo com as normas atuais e leis brasileiras vigentes.

1.4 OBJETIVOS

1.4.1 Objetivo Geral

Propor uma nova política de segurança da informação do Grupo X, a fim de melhorar a proteção das informações da organização, dos clientes e do público em geral tendo por base diretrizes técnicas e leis vigentes.

1.4.2 Objetivos Específicos

Para atender o objetivo final, faz-se necessário o desenvolvimento de objetivos pontuais que somados irão compor o objetivo principal:

- Propor uma nova política de segurança da informação, com foco na área de atuação da empresa;
- Adequar aos parâmetros de segurança que a Lei Geral de Proteção de Dados e as normas de Segurança da Informação exigem/sugerem;

1.5 ESTRUTURA DO TRABALHO

Este trabalho possui a estrutura apresentada na figura 1. Em seguida, descreve-se os conteúdos de cada etapa.

Figura 1 - Estrutura do trabalho

Fonte: O Autor, 2020.

Capítulo 1 - Introdução: Apresenta o tema, as delimitações da pesquisa, o problema, os objetivos da pesquisa, justificativa e os objetivos gerais e específicos.

Capítulo 2 – Referencial Teórico: Apresenta a estrutura base a ser aplicada durante o projeto de elaboração da nova Política, bem como um breve resumo das normas e Leis pesquisadas para a execução desse trabalho.

Capítulo 3 – Estudo de caso: Apresenta as políticas de segurança da informação (atual e a nova), fazendo uma análise comparativa entre ambas apontando as melhorias.

Capítulo 4 – Conclusão: Apresenta a conclusão após o desenvolvimento completo do trabalho, com os pontos de melhorias conquistados e as dificuldades encontradas durante o processo.

2. REFERENCIAL TEÓRICO

Será feito o levantamento e estudo de material normativo e legislativo que proverá suporte para a resolução dos possíveis problemas encontrados na política de segurança da informação do Grupo X, assim obtendo-se uma base sólida para a etapa seguinte de apresentação e validação da proposta.

A fundamentação teórica está estruturada com base nas normas da ABNT da família 27xxx e da lei geral de proteção de dados pessoais (LGPD), com o intuito de apresentar soluções técnicas aos problemas encontrados na etapa de apresentação da proposta, possibilitando a criação de documento dedicado à segurança da informação.

2.1 ISO 27001

Para a elaboração de uma política de segurança da informação consistente, é fundamental seguir as normas existentes na área. A ISO (*International Organization for Standardization*) é responsável pelas normas da família 2700x que apresentam os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gerenciamento de segurança da informação (SGSI) (ISO 27001, 2013).

O SGSI por sua vez fornece diversas diretrizes que quando seguidas trazem maior segurança durante o processo de tratamento da informação, garantindo assim que os riscos sejam gerenciados adequadamente preservando a confidencialidade, integridade e disponibilidade da informação.

Para a elaboração de uma SGSI é importante que a empresa aponte as questões internas e externas que são relevantes para a construção dessa SGSI (ISO 27001, 2013).

a) Equipes interessadas e relevantes para o sistema como um todo;
b) Os requisitos destas equipes – legais, regulamentares e/ou obrigações contratuais, para a segurança da informação.

Além de estabelecer a SGSI a organização deve estar comprometida com a implementação, manutenção e melhoria contínua deste sistema. A Alta Direção tem relação direta com a demonstração desse comprometimento, através de sua liderança, assegurando que a política de segurança da informação e os objetivos nela

propostos são compatíveis com as estratégias adotadas pela corporação, bem como os recursos para o SGSI estarão disponíveis possibilitando o alcance dos resultados pretendidos (ISO 27001, 2013).

Garantindo a integração do SGSI com os processos internos, pode-se observar o comprometimento da empresa com o sistema ao mesmo tempo que comunicando de maneira geral a importância do SGSI e orientando às pessoas que podem contribuir para a eficácia do sistema, cria-se uma atmosfera de cooperação que auxilia na aplicação das diretrizes propostas..

A política deve ser estabelecida levando em consideração o propósito da organização, incluindo ou fornecendo estrutura para o estabelecimento de objetivos de segurança da informação satisfazendo assim os requisitos relacionados à segurança, e ao mesmo tempo que apresenta o comprometimento com a melhoria contínua do SGSI documentando-a, comunicando-a internamente e disponibilizando-a a todas as partes interessadas (ISO 27001, 2013).

A definição de papéis por parte da Alta Direção da empresa, deve levar em consideração o *feedback* por parte da pessoa encarregada pela empresa para o processo de implantação, no que se refere ao desempenho do SGSI dentro da corporação, apresentando os resultados obtidos neste processo.

Quando avaliados os riscos de segurança da informação os mesmos auxiliam na compreensão dos problemas que podem ser gerados em caso de perda da confidencialidade da informação, e a avaliação destes riscos apresenta-nos à possibilidade de compensação para a mitigação desses riscos ou se o esforço não seria necessário por questão dos resultados apresentados.

Ao se estabelecer objetivos para a segurança da informação possibilita-se a atualização política e a mensuração dos resultados obtidos pela aplicação da mesma, esta mensuração pode ser realizada através dos parâmetros da norma ABNT 27004 (não faz parte do escopo deste trabalho). Estes objetivos devem ser documentados previamente no planejamento para que a corporação defina o que será feito em sequência e os recursos necessários para colocar em prática esse planejamento, bem como quem será o responsável pela execução do mesmo, e quando deverá estar concluído para que ocorra uma avaliação dos resultados (ISO 27001, 2013).

Prover os recursos necessários para todas as etapas da SGSI (estabelecimento, implementação, manutenção e melhoria contínua), são

responsabilidades da empresa, e a mesma deve observar a competência das pessoas no tratamento de suas atividades levando em conta a segurança da informação, e em caso de ausência do conhecimento necessário destas pessoas a empresa pode oferecer treinamentos ou as experiências necessárias para que essas pessoas consigam desempenhar suas atividades baseando suas tomadas de decisão na segurança da informação.

A conscientização do corpo de trabalhadores em relação à política da informação é de extrema importância, e também a relação da responsabilidade dos trabalhadores com o desempenho desta política, não deixando de lado as implicações no caso de não conformidade com os descritos na política (ISO 27001, 2013).

Conforme a norma o SGSI deve estar devidamente documentado, incluindo qualquer documentação adicional determinada como relevante para a eficácia do mesmo. A criação e controle de versões deve ser realizada visando a disponibilidade para o uso sempre que necessária, e garantido a proteção da integridade e confidencialidade, e também o armazenamento das mudanças realizadas em forma de versionamento (ISO 27001, 2013).

Os processos necessários para atender os requisitos de segurança da informação devem ser planejados e controlados, permitindo assim uma melhor avaliação e tratativa no que se refere a riscos de segurança da informação. Estas avaliações devem ocorrer de forma periódica e em casos de mudanças significativas nos processos que possam acarretar riscos à segurança da informação.

A avaliação de desempenho do SGSI deve ocorrer através de monitoramento e medição dos processos correlacionados, analisando e avaliando a eficácia do sistema. A definição de datas e papéis para estas realizações deve ser também apontada para que após o levantamento de informações e sua devida análise, se obtenha um status real da execução do SGSI, permitindo a correção em caso de desvio da forma mais rápida. As auditorias internas por sua vez, podem prover informações referentes a conformidade do SGSI com os requisitos da empresa para o sistema, e também com esta norma (ISO 27001, 2013).

A análise crítica por parte da direção da empresa, assegura a adequação, pertinência e eficácia do SGSI, e em caso de não conformidade pode apontar a necessidade de melhorias através de ações corretivas. Já a melhoria contínua auxilia o SGSI a manter-se atualizado com as normas e leis vigentes.

Alguns pontos servem como diretrizes para que a direção da empresa possa estabelecer uma PSI, segue:

- PSI de acordo com o propósito da organização;
- Fornecer estrutura para estabelecer os objetivos de segurança da informação;
- Apresente o comprometimento por parte da diretoria em satisfazer os requisitos que lhe cabe, relacionados com a segurança da informação;
- Apresente o comprometimento com a melhoria contínua;

2.2 ISO 27002

A Norma 27002 apresenta controles e diretrizes para serem aplicadas em organizações, ao mesmo tempo que permite o desenvolvimento destes para que melhor se adequem aos modelos de processos da empresa. Para o auxílio na criação de documentos como este é possível a utilização de referência cruzada, onde pode-se adaptar as diretrizes baseando as mesmas em um conceito contido nesta norma (ISO 27002, 2013).

Os seguintes pontos são de fundamental importância em qualquer PSI:

a) **Controle de Acesso**: Permitir ou não acesso a cada tipo de informação de acordo com a necessidade da função que o indivíduo executa, gerenciando a autorização, autenticação e a auditoria desses acessos;
b) **Classificação e Tratamento da Informação**: Com diversos tipos de informação, faz-se necessário a classificação da mesma por nível de confidencialidade – ex.: Confidencial, restrito uso interno e público;
c) **Segurança Física e do Ambiente**: Monitoramento e controles de acesso físico, possibilitando apenas a pessoas credenciadas, o acesso à locais onde tem o tratamento de informações mais restritas e/ou confidenciais;
d) **Tópicos Orientados à Usuários Finais** (uso dos ativos, boas práticas com a informação, dispositivos móveis no ambiente de trabalho, restrições a uso, transferência e manuseio, e também as restrições a instalação de softwares.): Criação e divulgação de manuais, instruções e material normativo, que esclareça os usuários finais, de como proceder

dentro do ambiente de trabalho, auxiliando assim a segurança da informação;

e) **Backup**: Definição de rotinas de criação, restauração e armazenamento de cópias de segurança, visando garantir a continuidade em caso de falhas sistêmicas, e/ou catástrofes climáticas;
f) **Proteção Contra *Malware***: Proteger e informar usuários no que se refere a *softwares* maliciosos, esclarecendo o que são e como identifica-los, além de proteger de forma eletrônica as informações da instituição;
g) **Vulnerabilidades Técnicas**: Identificar possíveis vulnerabilidades, e caso não as resolver, desenvolver ações para o tratamento e ou monitoramento, com o foco em garantir a continuidade do negócio;
h) **Controles Criptográficos**: Utilizar-se de criptografia no tráfego de informações, para garantir que em caso de extravio dessa informação a mesma seja ilegível a terceiros;
i) **Segurança nas Comunicações**: Gerenciamento e segurança dos serviços de redes, segregação das redes, políticas e procedimentos para transferência de informações inclusive acordos de confidencialidade e não divulgação;
j) **Proteção de Informações Referentes à Identificação Pessoal**: Orientar a empresa da importância do desenvolvimento e implementação de uma política de dados para a proteção e privacidade da informação de identificação pessoal.
k) **Relacionamento na Cadeia de Suprimento**: Esclarecer da necessidade de desenvolvimento e implementação de política referente ao tratamento junto a cadeia de suprimentos, tais como fornecedores, diretoria de tecnologia da informação (interna) e área de comunicação interna.

2.3 LGPD

A Lei Federal sob número 13.709 conhecida como Lei Geral da Proteção de Dados pessoais, regula a questão de tratamento de informações relacionada à pessoa natural identificada ou identificável não somente em meio físico, mas também em meio

digital, quando realizada por pessoa jurídica ou natural, e tem por objetivo proteger os direitos de liberdade e privacidade da pessoa física (BRASIL, 2018*)*.

A LGPD não foi projetada somente para os trâmites relacionados exclusivamente aos empregadores e empregados, mas para o uso do ambiente virtual/digital relacionado ao tratamento de informações dos cidadãos nas redes sociais, aplicativos e cadastros de clientes (OLIVIERI,2019). Ela também faz referência ao tratamento da informação de terceiros por parte de colaboradores em nome da empresa, podendo haver responsabilização em caso de má utilização dessas informações. Ou seja, é de suma importância a compreensão desta lei para o PSI, pois a relevância da proteção das informações passa de uma boa prática para o status de lei, obrigando a empresa a ter mais responsabilidade com os dados ao qual tem sob sua administração.

Como principais objetivos, a LGPD além de assegurar o direito à privacidade e proteção de dados pessoais, estabelece regras claras sobre a forma com esses dados devem ser tratados fortalecendo as relações jurídicas e a confiança do titular no tratamento dos dados pessoais, promovendo a livre concorrência e fomentando assim o desenvolvimento econômico e tecnológico.

A LGPD tem uma abordagem semelhante a um regulamento criado anterior a ela, na União Europeia. O Regulamento Geral de Proteção de Dados (GDPR), entrou em vigor em 2018 e regulamenta a proteção de dados de pessoas naturais por parte das empresas sediadas ou que atuem na União Europeia, determinando exigências sobre o uso de dados de terceiros. Ela apresenta diversas definições, responsabilidades e direitos por parte das pessoas naturais e jurídicas

A LGPD é apresentada da seguinte forma:

a) **Requisitos para o tratamento de Dados Pessoais**: Disserta sobre os termos cabíveis para a realização do tratamento dos dados pessoais, apresentando 3 seções distintas para o modo geral, os dados sensíveis e os dados de crianças e adolescentes;
b) **Término do Tratamento de Dados Pessoais**: Possui artigos voltados a explicitar as hipóteses onde ocorrem o término do tratamento de dados;
c) **Direitos do Titular**: Apresenta a qualificação que garante ao titular os direitos fundamentais de liberdade intimidade e privacidade, além de

direito de acesso à confirmação por parte do controlador do tratamento de seus dados, acesso aos seus dados, correção e informações referentes à possibilidade de não consentir com o tratamento de suas informações, bem como das consequências em caso de negativa;

d) **Regras e Responsabilidades do Tratamento de Dados Pessoais pelo Poder Público**: Expressa as regras e responsabilidades para o tratamento dos dados pessoais por parte do poder público, citando todas as leis que interajam com as situações descritas na Lei Geral de Proteção de Dados.
e) **Transferência Internacional de Dados**: Dispõe os casos em que a transferência de dados pessoais é permitida;
f) **Agentes de Tratamento de Dados Pessoais**: Indica as características e responsabilidades dos agentes envolvidos, esclarecendo os papeis do controlador e do encarregado e deixa aberta a possibilidade de estabelecimento de normas complementares por parte de autoridade nacional, e também disponibiliza os artigos que se referem ao ressarcimento de possíveis danos patrimoniais, morais, individuais ou coletivos;
g) **Segurança e Boas Práticas**: Apresenta boas práticas para o tratamento das informações pessoais bem como as medidas de segurança cabíveis;
h) **Fiscalização**: Expõe as sanções administrativas a serem aplicadas em razão a infrações cometidas às normas descritas na LGPD;
i) **Autoridade Nacional de Proteção de Dados e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade**: Discorre sobre a criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, mencionando sua composição e diretrizes de atuação;
j) **Disposições Finais e Transitórias**: Indica a data de vigência da lei assim como aponta a data de homologação e integraliza a lei as demais da República Federativa do Brasil.

A LGPD por sua vez entrou em vigor em agosto de 2020, e ofereceu um pouco mais de um ano para que as empresas nacionais pudessem entrar em conformidade com a lei (ISCHIARA, 2019).

2.4 ISO 27701

A ISO 27701 por sua vez fornece um direcionamento para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI). Ela apresenta essas diretrizes para os controladores de Dados Pessoais (DP) e operadores dessas informações (ISO 27701, 2019).

A extensão das diretrizes relacionadas à segurança da informação apresentadas na ISO 27002:2013, se deve ao fato de os dados pessoais serem afetados diretamente pelo SGPI por conta da LGPD. Neste caso é adicionado o sufixo ao termo Segurança da Informação, a fim de garantir também a sua privacidade e passando a ser reconhecida como segurança da informação e privacidade.

A criação de uma declaração da corporação em apoio e comprometendo-se a alcançar *compliance* com as leis e regulamentações vigentes, se faz necessária para o desenvolvimento ou em acréscimo a políticas de segurança da informação conforme quadro 1.

Quadro 1 - Seções Revisadas da ISO 27002

Seção da ABNT NBR ISO/IEC 27002:2013	**Título**	**Subseção neste documento**	**Comentários**
5	Políticas de segurança da informação	6.2	Diretrizes adicionais
6	Organização da segurança da informação	6.3	Diretrizes adicionais
7	Segurança em recursos humanos	6.4	Diretrizes adicionais
8	Gestão de ativos	6.5	Diretrizes adicionais
9	Controle de acesso	6.6	Diretrizes adicionais
10	Criptografia	6.7	Diretrizes adicionais

11	Segurança física e do ambiente	6.8	Diretrizes adicionais
12	Segurança nas operações	6.9	Diretrizes adicionais
13	Segurança nas comunicações	6.10	Diretrizes adicionais
14	Aquisição, desenvolvimento e manutenção de sistemas	6.11	Diretrizes adicionais
15	Relacionamento na cadeia de suprimento	6.12	Diretrizes adicionais
16	Gestão de incidentes de segurança da informação	6.13	Diretrizes adicionais
17	Aspectos da segurança da informação na gestão da continuidade do negócio	6.14	Sem diretrizes adicionais para o SGPI
18	*Compliance*	6.15	Diretrizes adicionais

Fonte: ISO, 2014.

a) **Políticas de Segurança da Informação**: Instrui quanto a criação de declaração de apoio e comprometimento com as regulamentações e legislações de DP (Dados Pessoais);
b) **Organização da Segurança da Informação**: Faz referência à necessidade de designação de um colaborador para ser o ponto focal quanto ao tratamento de DP, além de uma diretriz relacionada à necessidade de a empresa garantir a proteção dos dispositivos móveis para que não comprometam a segurança dos DP que a empresa tem sob sua guarda;
c) **Segurança em Recursos Humanos**: Adiciona a informação sobre a importância de instrução de membros relevantes da empresa, quanto à

relevância da privacidade dos DP, e o que pode comprometer caso sejam violadas;

d) **Gestão de Ativos**: Apresenta diretrizes adicionais nos quesitos de classificação da informação e tratamento de mídias, no que se refere à DP;
e) **Controle de Acesso**: Insere complementos em relação ao registro e cancelamento de usuários e no provisionamento de usuários, instruindo a instituição quanto à documentação e as possibilidades de responsabilização em alguns casos ao próprio cliente no que se refere a uso dos DP;
f) **Criptografia**: Algumas áreas requerem o uso de criptografia no trato de tipos específicos de DP. Convém que a organização forneça para o cliente as circunstâncias em que ela usa a criptografia para proteger os DP que ela trata;
g) **Segurança Física e do Ambiente**: Adiciona instruções quanto a reutilização ou descarte seguro de equipamento, bem como orientações quanto a políticas de mesa e tela limpa;
h) **Segurança nas Operações**: Apresenta diretrizes adicionais quanto às cópias de segurança e ao registro e monitoramento para operadores de DP;
i) **Segurança nas Comunicações**: Instrui as empresas quanto à criação de procedimentos para assegurar regras relativas ao tratamento de DP e também em relação a acordos de confidencialidade obrigatórios para indivíduos que operem DP que estão sob seu controle;
j) **Aquisição, Desenvolvimento e Manutenção de Sistemas**:
    1. Segurança de Sistemas de Segurança da Informação: Com relação a requisitos de segurança de sistemas de segurança da informação, convenciona que a transmissão de DP seja realizada de forma criptografada quando transmitidas por redes de dados não confiáveis. Estas redes podem ser tanto a própria internet pública quanto qualquer outra instalação fora do controle operacional da empresa.

2. Segurança em processos de Desenvolvimento e de Suporte: Sugere a adição de diretrizes em políticas de projetos de desenvolvimento de sistemas para garantir a proteção, definição das obrigações do titular e conformidade com a legislação vigente.
3. Dados para Teste: Adiciona alertas para que se evite a utilização de DP em testes, e caso não seja possível, que a empresa empregue nestes testes os mesmo métodos de segurança que possui no ambiente de produção, e em caso de impossibilidade sugere que haja uma seleção de controles para a mitigação de danos em caso de falhas.

k) **Relacionamento na Cadeia de Suprimento:** Implica na revisão e/ou ajustes de contratos junto a fornecedores, implicando na criação de controles que permitam a organização garantir que os DP tratados em todos os processos que envolvam fornecedores estejam seguros, conhecendo medidas aplicadas por parte do fornecedor para assegurar o *compliance* com as normas e leis vigentes.

l) **Gestão de Incidentes de Segurança da Informação:**
1. Responsabilidades e Procedimentos: Visa instruir a organização quanto à criação de documentos normativos que estabeleçam responsabilidade e procedimentos de identificação e registro em caso de violação de DP, além de processos que notifiquem as partes envolvidas nas violações de DP.
2. Resposta aos incidentes de Segurança da Informação: Apresenta exemplos para o tratamento de incidentes de segurança da informação, tanto para controladores de DP quanto para operadores de DP, incluindo formas de registrar e notificar as violações ocorridas com os possíveis efeitos destas violações.

m) **Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio:** Não ocorreram alteração de inclusão de diretrizes.

n) ***Compliance*:** Orienta a organização quanto à identificação de qualquer possibilidade de sanção legal resultante de alguma possível obrigação que tenha sido omitida em relação ao tratamento de DP, incluindo multas

substanciais oriundas diretamente da autoridade de supervisão local. Este documento poderá ser utilizado para formar uma base para contrato entre a organização e o cliente, estabelecendo as respectivas responsabilidades de proteção, segurança e privacidade dos dados pessoais.

3. ESTUDO DE CASO

O Grupo X atua na área de educação básica, de nível médio e superior. A instituição possui complexos de ensino por todo o Brasil, e atualmente possui aproximadamente 15 mil colaboradores.

Com uma diversificação dos perfis de usuários, há um grande desafio para a corporação manter a segurança das informações que estão sob sua guarda.

Sendo assim será realizado uma revisão no documento corporativo atual de segurança da informação, apresentando as inconsistências que afetam a segurança de dados de terceiros. A análise básica dos problemas da política atual serve para evidenciar os problemas encontrados durante a revisão da documentação institucional e após isso serão apontados pontos para a solução destes problemas.

Este documento proporá soluções de acordo com as leis vigentes na área e normas de segurança que quando aplicadas oferecem a proteção da integridade, sigilo e boa prática no tratamento destas informações, protegendo os proprietários destas informações.

3.1 ANÁLISE BÁSICA DOS PROBLEMAS DA POLÍTICA ATUAL (ANEXO 1)

A política de segurança da informação atual, utilizada pelo Grupo X até a presente data, não possui uma análise mais profunda da norma e deixa as diretrizes superficiais e pouco esclarecedoras. Outro problema que afeta o bom desempenho desta política, é a falta de atualização regular, pois esta desatualização deixa de adaptar a PSI às novas leis que entram em vigor para garantir a segurança dos proprietários das informações tratadas pela empresa, bem como os direitos da empresa para com o manuseio desta informação. É válido salientar que a LGPD foi criada após a data deste documento, entretanto este fato reforça ainda mais a necessidade de uma atualização constante.

A política antiga possui um glossário de conceitos resumido, reduzindo a quantidade de conceitos revisados e assim a capacidade de elucidação sobre assuntos atuais relacionados à segurança da informação, e generalizando alguns assuntos onde poderia ser obtido melhores resultados com uma pesquisa mais minuciosa sobre como proteger a informação, como: Multi Fator de Senha: Utiliza uma segunda forma (ou mais) de validação além da senha convencional. Essa outra forma

de validação pode ser feita por exemplo por biometria, reconhecimento facial ou até por um token gerado por aplicativo móvel instalado em dispositivo de acesso pessoal (celulares, tablets, etc.). e o Cofre de Senhas: Sistema de gerenciamento de senhas, que pode controlar os níveis de acessos, rastreando as ações executadas pela senha gerada, bem como quem solicitou esta senha ao sistema.

Em relação a documentação de referência onde se apresenta os documentos usados como base para a criação da política da empresa, observa-se que as fontes de pesquisas foram reduzidas e assim criou-se uma falsa sensação de seguimento das normas. Neste ponto pode-se observar também, que a estrutura utilizada de forma central na política foi prioritariamente baseada nos valores da instituição em detrimento às normas e leis, o que em caso contrário aproximaria a empresa de uma segurança da informação mais efetiva por se tratarem de pontos revisados e adotados em grande parte da comunidade internacional.

No que se refere às diretrizes a serem seguidas pelo corpo de colaboradores e terceiros, observa-se que as mesmas apresentam soluções muitas vezes genéricas e que não esclarecem pontos específicos o que aumentaria o grau de segurança dos dados da empresa. A falta de fiscalização (que pode ser observada pela mesma falta de atualização), deixa à desejar no quesito de melhoria contínua, barrando a evolução do documento, e principalmente do grau de comprometimento dos envolvidos com o tratamento da informação de forma responsável, deixando a classificação do nível de segurança das informações à mercê da interpretação ou bom senso do colaborador.

Tratando-se das diretrizes que apresentam em seu contexto as melhores práticas com relação a senhas e acessos, a negligencia com a atualização deixa de conhecer novos conceitos de segurança de acessos e com isso a empresa fica mais uma vez com um grande déficit de conhecimento.

3.2 ANÁLISE DOS PRINCIPAIS PONTOS ATUALIZADOS NO PROCESSO

Com a constatação dos pontos a serem melhorados na política antiga, a adequação da política nova deu-se através dos seguintes pontos principais apresentados na Figura 2.

Figura 2 - Principais pontos atualizados

Fonte: O Autor, 2020.

O processo de atualização iniciou-se com a leitura da documentação antiga (ANEXO 1), onde observou-se uma ausência de comunicação assertiva com o leitor mais leigo ao assunto o que atrapalha a empresa no alcance total aos seus colaboradores, tornando assim a política amplamente divulgada.

Com o intuito de aproximar a documentação de todos os tipos de leitores ao qual o documento seria exposto, foi desenvolvida uma apresentação no documento criado (item 3.3 deste documento), explicitando alguns pontos importantes para a compreensão da necessidade do mesmo, esclarecendo a relevância da informação nos dias de hoje e a importância de protege-la.

Esta apresentação explica também a importância de métodos que tornem a segurança da informação possível e a importância da fiscalização de execução destes métodos, informando ao leitor os conceitos de confidencialidade, integridade, autenticidade e disponibilidade.

Após este tópico foi observado os itens do glossário que apresentavam grande defasagem de informação em relação à termos que seriam abordados durante o documento. Estes foram considerados de grande importância para o conhecimento do leitor, permitindo ao mesmo durante a leitura destes termos no texto uma rápida compreensão do contexto em que o termo foi aplicado.

Com os termos técnicos mais claros foram complementadas as diretrizes, principal tópico do documento, inserindo e reescrevendo algumas para uma maior qualidade e alcance da diretriz. Em relação às diretrizes foi onde pode-se notar a indicação de diretivas técnicas que trazem inovação tecnológica em relação a política antiga.

As diretrizes de MFA (multi fator de autenticação) e cofre de senhas realizam uma atualização técnica de segurança muito importante atualmente, assim como a criptografia durante o trafego das informações de terceiros. A criptografia além de ser uma atualização tecnológica, faz parte das atualizações legislativas com relação a Lei geral de proteção de dados pessoais, e que determina a utilização da criptografia como forma de segurança deste tipo de informação.

Com a criação desta lei tornou-se necessária a atualização da política de segurança da empresa, como forma de adequação a lei, e a revisão das normas fez-se necessária tendo em vista que a norma também sofreu atualizações devido a nova lei.

Estas alterações estão presentes na nova política e foram desenvolvidas em busca de uma melhor compreensão e qualidade de execução de processos internos relacionados a execução de manuseio de informação de terceiros.

3.3 PROPOSTA DE NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Uma nova proposta de PSI deve levar em conta itens essenciais para obtenção de resultados efetivos. Para esta proposta foram observadas as leis atuais vigentes, e também as normas internacionais de padronização (família ISO 27xxx), mas não deixando de lado particularidades da empresa, possibilitando assim oferecer uma solução que se ajuste adequadamente ao ramo de atuação da corporação.

3.3.1 Apresentação

A informação é um ativo que possui grande valor para o Grupo X, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que visam garantir a segurança da informação que é prioridade constante na empresa, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a privacidade dos dados, os critérios éticos de pesquisa, a

imagem e/ou os objetivos da instituição, bem como oferecer segurança aos colaboradores, fornecedores e terceiros.

Como qualquer outro bem de uma instituição, a informação também precisa de proteção, principalmente se considerarmos aspectos como:

- A indisponibilidade da informação pode acarretar prejuízos para a instituição, gerando impactos financeiros para o grupo como um todo;
- Os dados e as informações de uso interno devem ser protegidos podendo resguardar a empresa em futuros investimentos relativos ao mercado externo;
- Dados com restrições internas, devem possuir controles que evitem o acesso de pessoas não autorizadas, dificultando a disseminação de informação restrita;
- Dados de terceiros devem possuir garantia de sua integridade e de que o acesso será realizado apenas por processos e/ou profissionais dependentes dessa informação para a execução de atividades pertinentes, devido ao fato de tratar-se de informações de clientes e fornecedores que necessitam de sigilo;
- Barreiras físicas com restrição de acesso a departamentos também devem ser observadas, pois pontos de controle de acesso possuem um papel importante dentro do sistema de segurança permitindo uma filtragem de todos que passam por esta etapa do processo, garantindo assim o mapeamento de quem segue adiante do processo e barrando pessoas que não necessitam ou não são permitidas a partir destes pontos de controle;

O Grupo X, em seu macroambiente considera que toda informação referente a suas estratégias e ações sejam resguardas, a fim de proteger a empresa.

Sendo assim, a forma como a informação é tratada dentro e fora da empresa vem corroborar com a constatação da necessidade da instituição em adotar, escrever, publicar, implementar e monitorar a política de segurança da informação (PSI), que é um instrumento importante para proteger a instituição contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade.

Apesar de não definir procedimentos específicos de uso, manipulação e proteção da informação, a Política de Segurança da Informação tem como objetivo definir direitos e responsabilidades para usuários, administradores de redes e sistemas, funcionários, gerentes e outros que lidam com a informação.

No entanto, apenas a criação e implantação da política não são suficientes se não existirem mecanismos de controle para assegurar que as normas estipuladas nessa política estão sendo efetivamente adotadas. Desta forma será necessário também elaborar e desenvolver tais mecanismos que podem ser implementados através de auditorias permanentes que terão como principal função verificar se as normas estão sendo efetivamente cumpridas. Tais normas não fazem parte deste estudo e deverão ser tratadas por normas ou regulamentos internos a serem desenvolvidos pela própria instituição.

Deve-se, ao elaborar a Política, considerar que a informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente em reuniões formais, em rodas de conversas, em mídias de áudio e de vídeo etc. Deve-se ainda considerar os seguintes aspectos básicos: confidencialidade, integridade, autenticidade e disponibilidade.

Deste modo esta política considera o fato de que a informação corporativa hoje se apresenta de várias formas e em diversas plataformas. Ainda também é válido frisar que independente do formato que se encontre a informação, a mesma estará coberta por esta política onde os pontos principais de cobertura referem-se à:

- Confidencialidade: Refere-se à privacidade dos dados tratados pela corporação. Esse conceito visa relacionar as medidas de segurança que resguardem as informações confidenciais e críticas contra qualquer tipo de evento que tente acessar, roubar e/ou alterar essas informações através de práticas ilegais;
- Integridade: Refere-se à necessidade de preservação das informações em seu estado natural, ao longo de todos os processos e sistemas ao qual ele seja submetido e/ou à preservação durante todo o ciclo de vida da informação dentro da empresa;
- Autenticidade: Consiste na garantia da veracidade ou originalidade, sendo necessário o cuidado e atenção no momento da inserção destas nos sistemas geridos pela empresa, além de métodos e processos que garantam a originalidade dos fatos mesmo quando o responsável por esta inserção for de fora da empresa;
- Disponibilidade: Refere-se ao fato de que a informação que uma empresa possui e/ou administra, necessita estar disponível sempre que necessário,

sendo garantida a acessibilidade aos colaboradores e sistemas que necessitam destas informações;

3.3.2 Objetivo

Aplicar diretrizes normativas e leis vigentes, a fim de garantir proteção das informações da organização, dos clientes e do público em geral seguindo diretrizes técnicas para o mesmo.

3.3.3 Abrangência / Nível de Distribuição

Esta política é aplicável para todos os colaboradores, irmãos, leigos e prestadores de serviços de todas as frentes de missão do Grupo X, ficando disponível eletronicamente nas intranets corporativas. A empresa, por sua vez, não consentirá com qualquer alegação de desconhecimento dos enunciados contidos nesta norma, por parte de ninguém à que ela se submeta, não importando as justificativas que poderão vir a ser apresentadas.

3.3.4 Siglas Utilizadas

CAD	Conselho de Administração
ABNT	Associação Brasileira de Normas Técnicas
NBR	Norma Técnica
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission

3.3.5 Glossário / Conceitos

Para melhor entendimento desta política, o quadro 2 apresenta uma definição reduzida de alguns conceitos utilizados:

Quadro 2 - Glossário

Acesso:	Ação de ingressar, transitar, conhecer, utilizar ou consultar ativos de informação de um órgão ou entidade.
Ameaça:	Conjunto de fatores e/causas em potenciais de um incidente, que podem resultar em dano para um sistema e/ou organização

Autenticação de Multifatores:	Utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema.
Ativos de informação:	Base de dados e arquivos, contratos e acordos, documentações de sistemas, informações sobre pesquisas, manuais de usuário, materiais de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas.
Backup ou Cópia de Segurança:	Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação destas informações, sendo uma cópia fiel à original. Pode ser também a mídia em que esta cópia é realizada.
Biometria:	Verificação de identidade de um indivíduo utilizando-se da validação de alguma característica física ou comportamental única, por meios automatizados;
Comitê de Segurança da Informação:	Comitê de Segurança da Informação: Grupo de pessoas com a responsabilidade de assessorar a implementação de ações de segurança da informação em uma instituição.
Compliance:	Se refere a promoção/execução de processos dentro de normas e padrões pré-estabelecidos, à fim de garantir uma qualidade destes processos
Confidencialidade:	Qualidade do processo em manter o sigilo das informações de terceiros ao qual a empresa está encarregada de armazenar para uso ou após o uso da mesma.
Continuidade de Negócios:	Garantia de sequência dos negócios da empresa, em caso de crises ou eventos que causem interrupção temporária das rotinas, geralmente através de um plano de recuperação e continuidade dos negócios;

Controlador:	Pessoa natural ou jurídica, a quem compete decisões referentes ao tratamento de dados pessoais;
Controle de Acesso:	Conjunto de procedimentos, recursos e meios utilizados para conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Normalmente requer procedimento de autenticação;
Criptografia:	Processo capaz de cifrar texto, com uso de processos computacionais previamente estabelecidos. O processo de decifragem do texto só poderá ser realizado através da chave de cifragem conhecida durante o processo de cifração ou outra que será gerada após o processo (caso de criptografia assimétrica).
Dados Pessoais:	Informação relacionada à pessoal natural identificada ou identificável.
Disponibilidade:	Propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda.
Engenharia Social:	Técnica utilizada para captura e/ou roubos de informação utilizando-se da ingenuidade e ou desconhecimento de normas por parte de colaboradores desatentos à segurança da informação, por meio desta técnica o indivíduo que tem interesse na informação utilizasse de persuasão para que a vítima execute tarefas e/ou forneça informações de interesse à ela.
Firewall:	Sistema de proteção por onde toda a informação é filtrada à fim de garantir que parâmetros de segurança sejam atendidos, possui o papel de evitar acessos não autorizados a uma determinada rede.
Incidente:	Evento, ação ou omissão, que permita ou possa permitir acesso não autorizado, interrupção ou mudança nas operações;
Informação:	Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode

	estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.
Integridade:	Propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental
Log:	Processo de registro de eventos relevantes em arquivo eletrônico de forma a possibilitar a rastreabilidade de transações informatizadas.
Negação de Serviço:	Bloqueio de acesso devidamente autorizado à um recurso ou atraso nas operações e funções normais de um sistema, o que resulta na perda de disponibilidade aos usuários. Geralmente são ataques aos recursos físicos dos servidores responsáveis pelo sistema, através de inúmeras solicitações falsas, que acarretam na sobrecarga dos equipamentos envolvidos;
Operador:	Pessoa física ou jurídica responsável pelo tratamento de dados pessoais em nome do controlador;
Phishing:	Ataques sem indivíduo alvo, visando “pescar” quem executar ações geralmente enviadas por meios de comunicação digitais, onde o atacante busca capturar informações pessoais para a execução de fraudes;
Requisitos de Segurança:	Conjuntos de necessidades que os sistemas (softwares e hardwares) devem atender à fim de garantir a segurança das informações que por eles trafegam;
Risco (em SI):	Potencial associado à exploração de vulnerabilidades de um ou mais ativos por parte de uma ameaça, com impacto negativo
Segurança da Informação:	Diz respeito à proteção de determinados dados, com a intenção de preservar seus respectivos valores para a Instituição ou um indivíduo. Podemos entender como informação todo o conteúdo ou dado valioso para um indivíduo/organização.
SI:	Acrônimo para sistemas da informação

Titular:	Pessoal natural à que se referem os dados pessoais que são objeto de tratamento;
Transferência de Risco:	Forma de tratamento de risco onde a empresa decide dividir o ônus do risco com um associado;
Vazamento de Dados:	Transmissão não autorizada de dados de dentro de uma organização para um destino ou recipiente externo. Pode ser intencional ou acidental e de forma física ou digital.

Fonte: Adaptado de Brasil, 2019.

3.3.6 Documentos de Referência

3.3.6.1 Referências externas

ABNT NBR ISO/IEC 27000:2014
ABNT NBR ISO/IEC 27001:2014
ABNT NBR ISO/IEC 27002:2014
ABNT NBR ISO/IEC 27701:2019
Lei Geral da Proteção de Dados Pessoais (*Lei nº 13.709, de 14 de agosto de 2018)*

3.3.6.2 Referências internas

- Política de Segurança da Informação (antiga);
- Código de Conduta do Grupo X
- Política de Consequências

3.3.7 Diretrizes

3.3.7.1 Colaboradores

- Todos os Colaboradores e prestadores de serviços do Grupo X devem assumir atitude de engajamento e responsabilidade com a proteção das informações do Grupo X;
- Os colaboradores devem compreender e possuir a capacidade de identificar as ameaças externas tais como vírus de computador, interceptação de mensagens eletrônicas e *phishing*;

- Assuntos confidenciais do Grupo X, não devem ser discutidos em ambientes públicos ou em áreas expostas (internas ou externas à instituição);
- As informações da instituição e/ou sob posse dela, devem ser utilizadas somente pela equipe/colaborador responsável pela mesma, ao mesmo tempo que a mesma só deve ser utilizada quando necessário para que o processo seja executado com excelência;
- A informação deve ser protegida durante todo seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte, podendo essa responsabilidade ser delegada à terceiros, mediante contratos protetivos que possibilitem um acompanhamento do Grupo X, caso solicitado, mediante ressarcimento por danos em caso do não cumprimento com as normas de segurança;
- A informação deve ser utilizada de forma responsável e apenas para a finalidade para a qual foi coletada;
- Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos em local apropriado;
- Os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, e ter documentação e planos de manutenção atualizados. O acesso irrestrito ao ativo da empresa, deve ser devidamente controlado e liberado apenas em caso previamente avaliados e com alta necessidade;
- Os ativos de informática e/ou eletrônicos corporativos devem possuir ferramenta de criptografia em seus discos rígidos, protegendo a informação em casos de perda e roubo;
- Todo ativo corporativo, é passivo de auditoria não devendo ser utilizado para fins particulares;
- As senhas com permissão de administrador devem ser obtidas através de sistema de cofre de senhas com atualizações diárias;
- A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento. As mesmas devem ser alteradas periodicamente;

- O processo de troca de senhas, necessita seguir alguns pontos de validação impossibilitando a solicitação da troca de senha por terceiros que não sejam os reais portadores da senha através de mecanismos de segurança como a validação multi fator (*multi factor authentication*);
- Senhas perdidas podem ser recuperadas apenas com validação do usuário (feita eletronicamente) ou por solicitação do gestor direto passível de validação eletrônica de igual forma;
- Somente softwares homologados pela Diretoria de Tecnologias e Sistemas, podem ser instalados nas estações de trabalho, e devem ser instalados exclusivamente pela equipe de serviços de informática;
- Tecnologias, marcas, metodologias e quaisquer informações que pertençam à Instituição não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho;
- As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes;
- O acesso às informações e recursos só deve ser realizado se devidamente autorizado;
- A identificação digital de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas através de sua identificação digital;
- A delegação de acessos deve seguir o critério de menor privilégio, no qual os usuários terão acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;
- Em períodos de transições temporárias de comando e ou atividades, o acesso necessário por esse período deve ser liberado e retirado ao seu final, devendo haver um monitoramento desses acessos temporários;
- Os acessos devem ser rastreáveis, à fim de garantir que todas as ações sejam passíveis de auditoria, possibilitando-se identificar individualmente o Colaborador para que seja responsabilizado internamente por suas ações;

- Todo acesso à informação do Grupo X que não tenha sido previamente autorizado é proibido;
- O Controle de acesso deve ocorrer durante todo o tempo de vida da informação e deve ser realizada tanto no âmbito digital como no controle de acesso físico;
    - No Caso do acesso físico, a validação biométrica pode ser utilizada para auxiliar no controle de acessos à ambientes mais restritos, aumentando assim a proteção de dados sensíveis;
- A Instituição deve promover a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação;
- Toda a divulgação que se refira à instituição deve ser aprovada previamente pelo departamento de Marketing e Comunicação;
- Todo processo da Instituição, deve garantir a segregação de funções, por meio da participação de mais de um Colaborador ou equipe de Colaboradores para o tratamento da informação;
- Os riscos às informações do Grupo X devem ser reportados através do canal de comunicação oficial disponibilizado, denominado Canal Direto, disponível em todos os sites da Instituição;
- Qualquer dúvida sobre esta Política de Segurança da Informação e suas normas deve ser esclarecida diretamente com o gestor direto e/ou com a área de Gestão de Segurança da Informação;
- O não cumprimento dessa política poderá acarretar sansões, que devem ser alinhadas com a Política de Consequências do Grupo X.

3.3.8 Estrutura De Segurança Da Informação Corporativa

3.3.8.1 Definição

A Estrutura de segurança da informação corporativa do Grupo X, é composta por um conjunto de documentos. Esses documentos são responsáveis por instruir e normatizar padrões de ações e comportamentos esperados por parte dos

colaboradores, quando se trata de manuseio de informações. Os documentos citados são:

- Política de Segurança da Informação;
- Política de Consequências;
- Código de Conduta;
- Normas de Segurança da Informação;
- Procedimentos de Segurança da Informação;
- Plano de contingência.

Política de Segurança da Informação: Define a estrutura, obrigações e diretrizes corporativas referentes à segurança da informação.
Políticas de Consequências: Rege no âmbito das sanções que poderão ser aplicadas em caso da não conformidade de ações do colaborador com as políticas de segurança. (*Este item não é alvo deste documento*)
Código de Conduta: Apresenta ao colaborador as diretrizes gerais da corporação, inclusive a necessidade de conhecimento de todas as políticas da instituição, e o seguimento das normas neles contidas. (*Este item não é alvo deste documento*)
Normas de Segurança da Informação: Estabelecem obrigações e procedimentos definidos conforme as diretrizes da PSI. (*Este item não é alvo deste documento*)
Procedimentos de Segurança da informação: Oferece material executivo conforme disposto nas normas da política, permitindo a aplicação na instituição. (*Este item não é alvo deste documento*)
Plano de Contingência: Apresenta procedimentos exclusivos para eventos de colapso de parte e ou total dos processos e equipamentos, visando uma rápida estabilização dos itens afetados. (*Este item não é alvo deste documento*)

3.3.8.2 Confidencialidade das Informações

O Grupo X possui próximo de 15 mil colaboradores e aproximadamente 40 mil clientes diretos. Com isso a confidencialidade das informações é um desafio diário. Podemos alcançar essa confidencialidade a partir de processos e ações seguras por parte dos envolvidos.

Todo dado pessoal solicitado pela instituição para utilização em seus processos deve ser armazenado, transferido e analisado de forma segura e em ambientes seguros (físico e/ou digitais), a fim de proteger a confidencialidade dessas informações

Esta PSI tem como principal objetivo a manutenção da confidencialidade e segurança das informações, atendendo a legislação atual. Por conta disso, esta PSI deverá ser revista sempre que houver qualquer alteração na legislação relacionada ao assunto, de forma a adequá-la as novas alterações, ou sempre que se julgue necessário devido a inovações tecnológicas e de processos que auxiliem em um melhor gerenciamento da segurança da informação.

3.3.9 Responsabilidades

Compreendendo que no Grupo X a informação é instrumento básico para o desenvolvimento de suas atividades, a Política de Segurança da Informação – PSI não pode basear-se exclusivamente em processos de restrição, mas sim deve atentar-se ao desenvolvimento de outras estratégias que garantam a sua abrangência de forma homogênea.

Uma forma de garantir a aceitação e replicação das diretrizes aplicadas neste documento, é envolver todos os colaboradores tornando-os responsáveis por:

- Cumprir a política de segurança do Grupo X, de maneira fiel;
- Em caso de dúvidas com relação a segurança da informação, buscar orientação do superior hierárquico imediato, para esclarecimento das mesmas;
- Assinar termo de responsabilidade, anuindo assim com as diretrizes dispostas na PSI, bem como assumindo a responsabilidade por seu cumprimento;
- Proteger as informações contra acessos, alterações, destruição e/ou divulgação não-autorizada pelo Grupo X;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Grupo X;
- Cumprir as leis e normas vigentes relacionadas à defesa de propriedade intelectual;

- Comunicar à área de Gestão da Segurança da Informação por qualquer descumprimento ou violação desta política e/ou normas e procedimentos a que ela se referencie.

Há também atribuições mais específicas além destes citados acima que são de ordem geral, que são direcionadas a setores responsáveis. Segue as atribuições específicas.

3.3.9.1 Diretoria do Grupo X

Destes setores com responsabilidades específicas, destaca-se a Diretoria do Grupo X. A ela cabe as seguintes atribuições:

- Aprovar a Política de Segurança da Informação e suas respectivas revisões;
- Aprovar a nomeação dos “proprietários” da informação;
- Tomar decisões administrativas referentes a descumprimentos da Política e/ou Normas encaminhados pelo Comitê Gestor de Segurança da Informação;
- Nomear membros para a criação deste Comitê Gestor;
- Dar autonomia para a equipe de auditoria interna executar fiscalização de qualquer membro do corpo de colaboradores, sob suspeita de extravio e/ou mal uso das informações sob responsabilidade da empresa.

3.3.9.2 Comitê de Gestão da Segurança da Informação

Outro setor relevante para a política de segurança da informação é um comitê de gestão da segurança da informação. Este setor tem as seguintes responsabilidades:

- Gerenciar e propor ajustes, aprimoramentos e modificações desta política;
- Aprovar normas de segurança da informação;
- Classificar as informações sob guarda e /ou pertencentes ao Grupo X;
- Analisar casos de violação desta política e das normas de segurança da informação, encaminhando-os a diretoria do Grupo quando for o caso;

- Propor projetos e iniciativas relacionadas à melhoria da segurança da informação do Grupo X;
- Planejar e alocar recursos financeiros, tecnológicos e humanos para garantir a segurança da informação;
- Solicitar relatórios, levantamentos e análises que forneçam as informações necessárias para auxiliar no processo de tomada de decisões;
- Fiscalizar o andamento de projetos e iniciativas com relação direta à segurança da informação;
- Classificar as informações, com níveis de risco quando necessário;
- Definir a relação de responsáveis das informações do Grupo X, relacionando o tipo de informação e a área que o administra;

Este comitê deverá conter membros das áreas relevantes da instituição, proporcionando assim uma direção mais assertiva e contemplando o ponto de vista de diversas frentes em relação à segurança da informação.

A formação do comitê poderá ser a seguinte:

- Presidente do Grupo X ou representante do gabinete da presidência;
- Diretor de auditoria, riscos e *compliance*;
- Diretor de tecnologia e sistemas;
- Gerente de Recursos Humanos;
- Diretor de Infraestrutura;
- Diretor de Marketing e Comunicação;

A coordenação das atividades exercidas pelo Comitê, caberá à Diretoria de Auditoria de Riscos e *Compliance* e pela Diretoria de Tecnologia e Sistemas, atividades estas relacionadas a convocações de reuniões e a realização de suporte as decisões tomadas em reuniões.

Todas as deliberações relacionadas à segurança da informação, devem passar por este comitê. Vale também ressaltar a importância de Reuniões Ordinárias com frequência mensal, mas não extinguindo a possibilidade de convocação de reuniões extraordinárias, levando em conta a necessidade de presença mínima de dois terços da composição total do comitê, para garantir a diversificação de pontos de vista em

relações aos assuntos pautados, garantindo um resultado mais homogêneo à nível institucional.

Será possível realizar o convite de terceiros para elucidação de assuntos mais profundamente, possibilitando aos votantes a compreensão do grau de importância de assuntos de fora de seu escopo de conhecimento. Estes convidados terceiros, não possuem direito a voto em assembleia.

3.3.9.3 Diretoria de Auditoria de Riscos e *Compliance*

A Diretoria de Auditoria de Riscos e *Compliance* (DARC), cabe as seguintes obrigações:

- Cumprir e fazer cumprir esta política, normas e procedimentos de segurança da informação;
- Avaliar todas as comunicações internas e externas, principalmente de forma proativa (antes de sua publicação) mas não deixando de observar as veiculadas de forma espontânea e em tempo real;
- Apontar desvios de conduta que comprometam a segurança da informação ao comitê de gestão da segurança da informação;
- Auditar processos de segurança e apontar pontos de observação para futuras melhorias, ao comitê de gestão de segurança da informação;

3.3.9.4 Diretoria de Tecnologia e Sistemas

Com a atualização constante de mecanismos de tecnologia para a segurança da informação, a Diretoria de Tecnologia e Sistemas, tem um papel importante em relação à proteção da informação. Segue as responsabilidades específicas:

- Cumprir e fazer cumprir esta política, normas e procedimentos de segurança da informação;
- Avaliar a utilização dos sistemas e recursos de tecnologia, com o intuito de garantir a sua interoperabilidade, com relação a sistemas de segurança da informação, fornecendo permanente disponibilidade dos dados e assegurando a proteção dos mesmos;

- Propor projetos e iniciativas relacionados a melhorias da segurança da informação do Grupo X, mantendo-se atualizada em relação às melhores práticas e tecnologias disponíveis;
- Prover todas as informações de gestão da segurança da informação sempre que solicitadas pelo comitê de gestão da segurança da informação;
- Estabelecer controles de acesso físicos e/ou lógicos, com a função de proteger recursos tecnológicos e arquivos de dados contra perda, modificação ou divulgação não autorizada;
- Manter arquivos de log que registrem as ações dos usuários, à fim de serem fontes de informação para auditorias futuras;
- Ofertar orientação e treinamento sobre a política de segurança da informação e suas normas as todos os colaboradores do Grupo X;
- Gerenciar sistemas de controle de acesso, incluindo concessão, manutenção, revisão e suspensão de acessos aos usuários;
- Analisar e tratar riscos relacionados à segurança da informação do Grupo X, além de apresentar relatórios periódicos sobre tais riscos ao comitê de gestão da segurança da informação, apresentando propostas de aperfeiçoamento da segurança da informação para tais riscos;
- Realizar testes de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas e ambientes em que circulam as informações do Grupo X;
- Estabelecer mecanismos para registro e controle de não conformidade a esta política e as normas de segurança da informação, comunicando o comitê de gestão da segurança da informação.

3.3.9.5 Diretoria de Recursos Humanos

Esta diretoria tem grande responsabilidade no que se refere à responsabilidade com as informações dos próprios colaboradores da empresa. As responsabilidades deste setor são:

- Cumprir e fazer cumprir esta política, normas e procedimentos de segurança da informação;
- Oferecer orientação e treinamentos sobre a política de segurança da informação e suas normas a todos os colaboradores do Grupo X;
- Colher termos de responsabilidades dos colaboradores, devidamente assinados, arquivando-os junto ao registro do mesmo;
- Trabalhar em conjunto com outras diretorias, nos informes referentes a desligamentos, afastamentos, licenças e férias, para que as outras áreas possam realizar os procedimentos referentes à acessos físicos e digitais, resguardando sempre os dados da empresa.

3.3.9.6 Diretoria de Infraestrutura

Como responsável pela segurança patrimonial, a Diretoria de Infraestrutura cabe:

- Cumprir e fazer cumprir esta política, normas e procedimentos de segurança da informação;
- Monitorar acessos físicos em toda planta da empresa;
- Reportar atividades suspeitas em tempo real, e abordar terceiros estranhos ao ambiente;
- Realizar averiguações através de arquivos de sistema de monitoramento, para elucidação de qualquer suspeita de roubo ou perda de informação, e ou equipamentos e recursos que possuam características de armazenamento da mesma;
- Operar sistemas de monitoramento para controle de acesso, inclusive na falha de algum sistema, operar com recursos humanos até o retorno dos sistemas.

3.3.9.7 Diretoria de Marketing e Comunicação

Cabe a diretoria de marketing e comunicação:

- Cumprir e fazer cumprir esta política, normas e procedimentos de segurança da informação;

- Avaliar e liberar publicações de conteúdos nos canais internos e externos, observando as diretrizes da política e as normas de segurança da informação;
- Promover ampla divulgação da política e das normas de segurança da informação de forma a atingir todos os colaboradores do Grupo X.

A todas as Diretorias é importante também assegurar-se de:

- Cumprir e fazer cumprir, dentro de suas atribuições, o disposto nas Leis vigentes.

3.4 ANÁLISE DE ADEQUAÇÃO DA NOVA POLÍTICA

A adequação da nova política tomou por base as normas ABNT da família 27XXX, a Lei Geral de Proteção de Dados Pessoais e a política de segurança da informação antiga.

Além de uma atualização da política devido ao tempo em que a mesma foi criada - o que pode significar muitas mudanças devido ao fato das atualizações tecnológicas possuírem a possibilidade de um avanço gigantesco em um curto período de tempo, foi abrangida uma nova lei que adequa a empresa legalmente falando em relação ao tratamento de dados pessoais.

No início da nova política foi dado um contexto em relação à natureza do documento (PSI) e uma apresentação sobre a importância da informação para a instituição, inclusive um breve resumo dos pontos focais de segurança da informação. Apresenta-se também uma descrição dos pilares da segurança da informação, definindo-os de forma sucinta e clara.

Após a pontuação do objetivo e abrangência, o documento traz além das siglas utilizadas, um glossário de conceitos mais robusto que o que havia na política antiga, muitos dos pontos apresentados aqui devem-se ao fato da atualização tecnológica durante o período de ausência de atualização, outros porém são conceitos preexistentes que faltavam no documento antigo, o que poderia acarretar em interpretações erradas do documento por falta de conhecimento técnico em relação aos termos utilizados na transcrição do documento. É importante salientar que um glossário robusto por si só não enriquece o documento se apenas são apresentados conceitos aleatórios sem fundo prático. Tendo isso em mente a intenção foi trazer conceitos inerentes ao assunto e presentes de alguma forma na constituição do

documento, visando conscientizar o leitor em relação aos temas descritos em cada diretriz constante na sequência do material.

Com a referência buscou-se ampliar a base técnica de pesquisa, utilizando as normas da família 27xxx de uma forma um pouco mais ampla, e absorvendo os conteúdos para a compreensão da forma de apresenta-lo ao colaborador leigo. Além disso essa pesquisa possibilitou a contextualização dos problemas da empresa, com a norma, permitindo a realização de um filtro mais fiel às necessidades reais da empresa.

Em relação a Lei Geral da Proteção de Dados Pessoais (um dos pontos principais para o desenvolvimento desta política), foi apresentado totalmente de forma nova ao documento, e sua importância legal está marcada nas diretrizes. Como esta lei é relativamente nova, ela serve como guia para a elucidação de muitos pontos referentes a manipulação e armazenamento de informação não pertencentes a empresa, mas que são cruciais para a execução de processos internos.

No Capítulo sobre estrutura de segurança da informação corporativa, apresenta-se uma breve definição seguido de uma série de documentos auxiliares que se desenvolvidos e aplicados pela empresa podem aumentar a eficácia da política de segurança da informação em relação às condutas esperadas, possíveis consequências, normas internas a serem seguidas e planos de redução de perdas em “catástrofes”.

Após as diretrizes ainda temos as responsabilidades inerentes a cada setor e trabalhador envolvido nos processos corporativos, nesse ponto são apresentadas as responsabilidades de forma segmentada, permitindo aos responsáveis por cada área a identificação imediata de sua responsabilidade dentro do processo de segurança da informação.

Por fim as diretrizes globais, apresentam as normas a serem aplicadas após a implementação desta política. Com a atualização deste documento, sugere-se o acompanhamento por equipe dedicada durante a sua implementação no caso de haver necessidades especiais relevantes à política, para que possam ser inclusas em uma nova versão, e também a fiscalização da aplicação da política como parte de todos os processos.

Levando em conta que é recomendado ser a mesma equipe que faz esses apontamentos e realiza a fiscalização, a mesma pode se preparar melhor para uma

atualização após 6 meses de prática, com esta equipe atenta a atualizações tecnológicas, normativas e de cunho legal, a fim de tornar a prática de melhoria contínua uma apoiadora da segurança da informação.

4. CONCLUSÃO

A partir da necessidade legal de proteção de dados pessoais, este trabalho realizou a atualização da política de segurança de uma grande empresa adequando-a as leis atuais vigentes, além de realizar uma atualização nas diretrizes de segurança seguidas pela empresa anteriormente.

Para tornar esse trabalho possível, foi realizada uma pesquisa dentro das normas de segurança da ABNT/ISO da família 27xxx que são designadas para o estabelecimento, implementação, manutenção e melhoria de um sistema de gerenciamento de segurança. Porém como o foco principal deste trabalho era o de adequar a política de segurança a atenção primária foi focar na adequação, mas não deixando-se de utilizar as normas diretivas contidas em todo o material que também engloba a criação/ melhoria de política de segurança da informação.

Este trabalho também trouxe a nova política, a inserção das obrigatoriedades referentes a Lei Geral da Proteção de Dados Pessoais, o que concilia as necessidades legais, com as boas práticas de segurança da informação contidas nas Normas.

Além do enriquecimento do documento adequado, com informações mais completas ao ter-se uma base de pesquisa mais profunda, a criação de um documento a ser seguido por uma instituição possibilitou a visualização de problemas complexos, que podem ocorrer por simples práticas incorretas, que muitas vezes podem acontecer por falta de conhecimento das leis e práticas eficientes de controle de ações. Com isso uma visão mais ampla dos compromissos da empresa com os clientes, colaboradores e fornecedores, vai além de somente uma prestação de serviço, mas acarreta no comprometimento da mesma com todo o processo de segurança das informações sob sua responsabilidade, pelo tempo em que necessita ficar sob posse dessas informações para seu uso.

Outro ponto conhecido também, foi referente à responsabilidade legal da empresa pelas ações de seus colaboradores em relação às informações manuseadas, o que enfatiza ainda mais a necessidade desta adequação. Com a reeducação do corpo de colaboradores, através de programas de disseminação de conhecimentos, normas e incluso esta política, pode-se reduzir as possibilidades de má conduta e extravios de informações críticas simplesmente restringindo acessos desnecessários, educando

sobre boas práticas durante o manuseio dessas informações, e direcionando o colaborador por um caminho seguro para a execução de seu trabalho.

Conclui-se também que a realização desta adequação deve ser contínua, possibilitando uma atualização de forma menos desgastante do ponto de vista do colaborador que necessita absorver as mudanças, mas também permitindo uma adequação mais suave pois depende apenas das atualizações realizadas no período entre a última e a próxima atualização.

Durante algumas etapas deste trabalho foram encontradas dificuldades que não chegaram a parar o processo, porém atrasaram o levantamento de conteúdo transformando a pesquisa e criação em atividades mais lentas e demoradas.

A primeira dificuldade real encontrada durante o processo, foi a liberação da empresa para uso e citação da sua marca durante o processo de estudo. A dificuldade não foi vencida totalmente nesse caso (a empresa não foi mencionada durante o trabalho devido a esta situação), neste ponto o contato com colaboradores internos mostrou-se lento e ineficaz – mesmo considerando o fato de conhecê-los pessoalmente, pois mesmo chegando à pessoa responsável pela política de segurança com a indicação direta do Diretor de Auditoria, a demora de respostas e reenvio de e-mails tornou a comunicação inviável devido à falta de interesse por parte dos colaboradores responsáveis pela atual política (a espera por retorno a cada *e-mail* enviado se dava entorno de 2 semanas).

O acesso a política interna se deu devido ao fato de ter colaboradores solícitos que repassaram a documentação a mim, com isso foi possível realizar a ocultação e utilização do material isentando totalmente a empresa de qualquer ônus.

Outro ponto que impactou negativamente o processo de execução deste trabalho, foi o fato de o assunto ser muito atual, o que a principio poderia parecer um ponto positivo, pois várias informações poderiam ser encontradas, mas se se provou um processo de grande dificuldade, devido à falta de referências confiáveis sobre o assunto. A parte normativa e legislativa foi de fácil acesso como o esperado, porém ao buscar casos, citações e explicações sobre o tema central, muito do material encontrado não estava vinculado a fontes confiáveis.

Ao fim conseguiu-se filtrar as fontes e obtê-las através de periódicos e *journals* renomados mundialmente, para trazer um conteúdo mais fidedigno a realidade do assunto atualmente.

REFERÊNCIAS

ABNT. **Conheça a ABNT.** Disponível em: <http://www.abnt.org.br/abnt/conheca-a-abnt>. Acesso em 01 abr. 2019.

AGÊNCIA O GLOBO. **Brasil é o país mais vulnerável a vazamento de informações, diz pesquisador.** 14 set. 2017. Disponível em: <https://revistapegn.globo.com/Tecnologia/noticia/2017/09/brasil-e-o-pais-mais-vulneravel-vazamento-de-informacoes-diz-pesquisador.html> Acesso em 21 mar. 2019.

ANDRADE, Alex Sales. **Segurança da informação com foco em infraestrutura: um estudo de caso em uma empresa do setor de tecnologia da informação.** Monografia (Bacharelado em Ciência da Computação). Universidade Federal de Lavras, Lavras, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023: Informação e documentação: Referências**. Rio de Janeiro, p. 24. 2002.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação. **Glossário de Segurança da Informação**. Diário Oficial da União. 190 ed. seção 1, p. 3, 01 out. 2019.

CAMARGO, Robson. **Ciclo de vida de um projeto: tudo que você precisa saber para ter sucesso.** Robson Camargo projetos e negócios, gerenciamento de projetos, 02 abr. 2019. Disponível em: <https://robsoncamargo.com.br/blog/Ciclo-de-vida-de-um-projeto>. Acesso em 07 dez 2019.

CLIMA COMUNICAÇÃO. **A comunicação interna entra na formação da cultura e do clima organizacional?** 01 ago. 2019. Disponível em: <https://blog.climacomunicacao.com.br/cultura-e-clima-organizacional/>. Acesso em 05 dez. 2019.

COSTA, L. N.; A importância de uma política dinâmica de segurança da informação em uma empresa de grande porte. 2014. 67f. Monografia de especialização – Universidade Tecnológica Federal do Paraná, Curitiba, 2014.

EFE. **Uber escondeu roubo de dados de 57 milhões de pessoas**. Revista Exame, 21 nov. 2017. Negócios. Disponível em: <https://exame.com/negocios/uber-escondeu-roubo-de-dados-de-57-milhoes-de-pessoas/>. Acesso em 16 jun. 2020.

HSC BRASIL. **Conheça 7 boas práticas de segurança da informação para empresas**. 06 ago. 2018. Disponível em: <https://www.hscbrasil.com.br/boas-praticas-de-seguranca-da-informacao/>. Acesso em 05/12/2019.

INTERNATIONAL STANDARD ORGANIZATION. **ISO/IEC 27000: *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*** Suíça, p. IV. 2014.

ISCHIARA, Michele. **Quais as semelhanças e diferenças entre a LGPD do Brasil e GDPR da UE?** CIO, 08 jul. 2019. Gestão. Disponível em: < https://cio.com.br/quais-as-semelhancas-e-diferencas-entre-a-lgpd-do-brasil-e-gdpr-da-ue/>. Acesso em 01 mar. 2020.

ISO. **The ISO Story.** Disponível em: <https://www.iso.org/the-iso-story.html>. Acesso em 01 abr. 2019.

JUNIOR, Carlos**. Ciclo PDCA: uma ferramenta imprescindível ao gerente de projetos!** Project Builder, 30 mai. 2017. Disponível em: <https://www.projectbuilder.com.br/blog/ciclo-pdca-uma-ferramenta-imprescindivel-ao-gerente-de-projetos/>. Acesso em 06 dez. 2019.

KENOBY. **Comunicação interna: conheça a importância para a sua empresa.** 25 FEV. 2019. Disponível em: <http://www.kenoby.com/blog/comunicacao-interna/>. Acesso em 07 dez. 2019.

KHAIRA, Rachna. **Rs 500, 10 minutes, and you have access to billion Aadhaar details.** The Tribune, Nation, 04 jan. 2018. Disponível em: <https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html>. Acesso em 01 dez. 2019.

LOUSADA, M.; VALENTIM, M. L. P. Modelos de tomada de decisão e sua relação com a informação orgânica. **Perspectivas em Ciência da Informação**, v. 16, n. 1, p. 147-164, 2011. Disponível em: <http://hdl.handle.net/20.500.11959/brapci/32244>. Acesso em: 04 jan. 2020.

MACHADO, Marcel Jacques. **Controle de acessos.** 04 fev. 2017. Disponível em: <https://marceljm.com/seguranca-da-informacao/controle-de-acessos/>. Acesso em 02 dez. 2019.

MELLO K., TEIXEIRA L. B. Por que estamos na era da proteção da informação. **Forbes.** 01 jan. 2019. Negócios. Disponível em: <https://forbes.uol.com.br/negocios/2019/01/por-que-estamos-na-era-da-protecao-da-informacao/>. Acesso em 05 abr. 2019.

NEOTRIAD. **Entenda a importância da comunicação interna nas organizações.** 21 JUL. 2016. Disponível em: <https://gestaodeequipes.com.br/entenda-a-importancia-da-comunicacao-interna-nas-organizacoes/>. Acesso em 02 dez. 2019.

NORMAS TÉCNICAS. **Série ISO 27000.** Disponível em: <https://www.normastecnicas.com/sem-categoria/serie-iso-27000/>. Acesso em 02 dez. 2019.

OLIVIERI, Nicolau. **Rotinas e contratos de trabalho serão impactados pela LGPD?** 30 out. 2019. Disponível em: <http://www.serpro.gov.br/lgpd/noticias/impactos-lgpd-rotinas-trabalhistas-contrato-de-trabalho >. Acesso em 04 dez. 2019.

PACHECO, A. C. Gestão de projetos tem importância estratégica para as empresas. **Revista IETEC**, nº 51. Belo Horizonte, jun. 2013. Disponível em: <http://www.techoje.com.br/site/techoje/categoria/detalhe_artigo/1739>. Acesso em: 30 mai. 2019.

PALMA, Fernando. **O que é um Sistema de Gestão de Segurança da Informação (SGSI)**. Disponível em: <https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html>. Acesso em 02 dez. 2019.

PIONTI, R. **Política de Segurança da Informação – Conceitos, Características e Benefícios.** Disponível em: <https://www.profissionaisti.com.br/2013/08/politica-de-seguranca-da-informacao-conceitos-caracteristicas-e-beneficios/>. Acesso em: 30 mai. 2019.

POSITIVO TECNOLOGIA. **A importância da gestão da informação para o sucesso de um negócio**. Gestão, 25 mar. 2019. Disponível em: <https://www.meupositivo.com.br/panoramapositivo/gestao-da-informacao/>. Acesso em 01 dez. 2019.

REVISTA EXAME. **62% da população brasileira está ativa nas redes sociais.** 19 out. 2018. Disponível em: <https://exame.abril.com.br/negocios/dino/62-da-populacao-brasileira-esta-ativa-nas-redes-sociais/>. Acesso em 21 set. 2019

ROCHA, F. L. **Ciclo de Vida de Projeto.** 13 jul. 2013. Gerenciamento de Projetos. Disponível em: <https://felipelirarocha.files.wordpress.com/2013/07/imagem2_ciclodevida2.png>. Acesso em: 01 abr. 2019.

SANTOS, V. F. M. **O que é o Ciclo de vida de um projeto?** FM2S, Gestão de projetos, 06 jun. 2017. Disponível em <https://www.fm2s.com.br/ciclo-de-vida-projeto/>. Acesso em 07 dez. 2019.

SILVA A. **Implantação do Projeto de Gestão de Segurança da Informação.** 23 NOV. 2011. Disponível em: <https://administradores.com.br/artigos/implantacao-do-projeto-de-gestao-de-seguranca-da-informacao>. Acesso em: 30 mai. 2019.

TEIXEIRA, Marcelo. Petrobras confirma roubo de computadores com dados importantes. **Reuters**, São Paulo, 15 fev. 2008. Notícias de negócios. Disponível em: <https://br.reuters.com/article/internetNews/idBRN1443347020080215>. Acesso em 21 mar. 2019.

TREVISAN, Nanci. **Comunicação organizacional em tempos de mídias sociais.** Implantando Marketing, artigos e comunicação, 12 nov. 2018. Disponível em: <https://www.implantandomarketing.com/comunicacao-organizacional-em-tempos-de-midias-sociais/>. Acesso em 04 dez. 2019.

WAKKA, Wagner. **Prosegur é alvo de ataque ransomware e precisa parar suas operações**. Canaltech, 29 nov. 2019. Segurança, hacker. Disponível em: <https://canaltech.com.br/hacker/prosegur-e-alvo-de-ataque-ransomware-e-precisa-parar-suas-operacoes-156717/>. Acesso em 16 jun. 2020.

ANEXO 1 - POLITICA ATUAL

Como ponto de partida para a execução deste trabalho segue a política de segurança atual do Grupo X, que serve como referência para a criação de um novo modelo mais robusto, atualizado as normas e leis vigentes.

OBJETIVO

Estabelecer a Política de Segurança da Informação do Grupo X à luz dos valores institucionais, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações da organização, dos clientes e do público em geral.

ABRANGÊNCIA / NÍVEL DE DISTRIBUIÇÃO

Esta política é aplicável para todos os colaboradores, irmãos, leigos e prestadores de serviços de todas as frentes de missão do Grupo X, ficando disponível eletronicamente nas intranets do Grupo X.

O Grupo, por sua vez, não consentirá com qualquer alegação de desconhecimento dos enunciados contidos nesta norma, por parte de ninguém a que a ela se submeta, não importando as justificativas que poderão vir a ser apresentadas.

SIGLAS UTILIZADAS

CAD	Conselho de Administração

GLOSSÁRIO / CONCEITOS

Para melhor entendimento desta política, os seguintes conceitos são utilizados:

Ativos de informação	Base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de

	recuperação, trilhas de auditoria e informações armazenadas.
Informação	Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.
Segurança da Informação	Diz respeito à proteção de determinados dados, com a intenção de preservar seus respectivos valores para a Instituição ou um indivíduo. Podemos entender como informação todo o conteúdo ou dado valioso para um indivíduo/organização.
Princípios de Segurança da Informação	confidencialidade - Garante que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário;

DOCUMENTOS DE REFERÊNCIA

Referências externas

ABNT NBR ISO/IEC 27001:2013 Sistemas de gestão da segurança da informação.

Referências internas

Código de Conduta do Grupo X

Política de Consequências

DIRETRIZES

As informações da Instituição, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

A informação deve receber proteção adequada em observância aos princípios e diretrizes da Instituição em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

A informação deve ser utilizada de forma responsável e apenas para a finalidade para a qual foi coletada.

Todo processo da Instituição, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um Colaborador ou equipe de Colaboradores.

Os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, e ter documentação e planos de manutenção atualizados.

O acesso às informações e recursos só deve ser feito se devidamente autorizado.

A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.

Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, para que seja responsabilizado por suas ações.

A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

Tecnologias, marcas, metodologias e quaisquer informações que pertençam à Instituição não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes.

A Instituição deve promover a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação.

Os riscos às informações do Grupo X devem ser reportados através do canal de comunicação oficial disponibilizado, denominado Canal Direto, disponível em todos os sites da Instituição.

Esta Política de Segurança da Informação é complementada por normas específicas de Segurança da Informação (circulares SI, integrantes do conjunto de normativos do Grupo X em conformidade com os aspectos legais e regulamentares aprovados pela Instituição).

O não cumprimento dessa política poderá acarretar sansões, que devem ser alinhadas com a Política de Consequências do Grupo X.

RESPONSABILIDADES

Conselho de Administração

• Aprovar formalmente a política de Segurança da Informação, assim como quaisquer futuras revisões;

• Deliberar as estratégias de segurança da informação bem como a alocação de recursos e priorizações dos trabalhos.

Diretor Presidente

• Facilitar comunicação aberta e direta com todos os executivos;

• Manter fluxo de informação sobre novas atividades, iniciativas e negócios;

• Assegurar ao Diretor de Auditoria, Riscos e *Compliance* os recursos e acessos necessários para a execução de suas responsabilidades;

• Apoiar o Grupo X para a condução de controles de Segurança da Informação efetivo (alocação de recursos, priorizações, etc.).

Superintendência e Diretorias Executivas

• Contribuir nas atividades de identificação e avaliação dos riscos de segurança da informação inerentes aos processos de negócio sob sua responsabilidade.

• Implementar os planos de ação e acompanhar as atividades corretivas e/ou preventivas nos processos sob sua responsabilidade.

• Atentar-se para conduzir suas atividades de acordo com as diretrizes estabelecidas pelas políticas vigentes no Grupo X, bem como as melhores práticas de governança.

Diretoria de Auditoria Interna, Riscos e *Compliance* – DARC

• Assegurar a manutenção da política de Segurança da Informação e verificar o cumprimento das diretrizes estabelecidas;

• Contemplar o tema de Segurança da Informação em seu escopo de treinamentos de conscientização;

• Manter equipe de auditores capacitados, periodicamente atualizados e com experiência adequada ao cumprimento dos requerimentos desta política e boas práticas;

Diretoria de Tecnologia e Sistemas – DTS

• Suportar as atividades técnicas que visam suportar o Grupo X em controles

preventivos e detectivos;

• Manter os sistemas e equipamentos atualizados, bem como a equipe capacitada a fim de evitar incidentes de segurança da informação em situações que possam ser remediadas antecipadamente.

Profissionais que trabalham no Grupo X

• Conduzir suas atividades de acordo com as diretrizes estabelecidas pelas políticas vigentes no Grupo X, bem como as melhores práticas de governança.

• Reportar diretamente para o Gestor de sua área sobre eventuais atividades que possam colocar o Grupo X em risco.

DA VIGÊNCIA

A presente Política de Segurança da Informação entra em vigor a partir de 01 de janeiro de 2018.

HISTÓRICO DE ALTERAÇÕES DO DOCUMENTO

HISTÓRICO DE ALTERAÇÕES	DESCRIÇÃO (item alterado)
10/11/2017	Emissão do documento