RILCO
ISSN 2695-6098
https://doi.org/10.51896/rilcods
DESARROLLO SUSTENTABLE, NEGOCIOS, EMPRENDIMIENTO Y EDUCACIÓN
latindex Dialnet IDEAS

A QUALIDADE DA INFORMAÇÃO EM UM SISTEMA DE GESTÃO DE SEGURANÇA (ISMS) ATRAVÉS DE UM SOFTWARE BASEADO NA PADRÃO ISO 27001 PARA INSTITUIÇÕES DE EDUCAÇÃO, MÉXICO, 2021

Juan Alberto Ruíz Tapia[1]
Susana Ruíz Valdés[2]
César Enrique Estrada Gutiérrez[3]

Para citar este artículo puede utilizar el siguiente formato:

Juan Alberto Ruíz Tapia, Susana Ruíz Valdés y César Enrique Estrada Gutiérrez (2021): "A qualidade da informação em um sistema de gestão de segurança (ISMS) através de um software baseado na padrão iso 27001 para instituições de educação, México, 2021", Revista de Desarrollo Sustentable, Negocios, Emprendimiento y Educación RILCO DS, n. 26 (p.p. 64-81, diciembre 2021). En línea:
https://www.eumed.net/es/revistas/rilcoDS/26-diciembre21/sistema-seguranca

RESUMO

O objetivo desta pesquisa foi criar um aplicativo computacional para melhorar a qualidade da informação aplicada às instituições de ensino com base na norma ISO 27001. Tem como objetivo reduzir os riscos do computador e propor um plano de tratamento de riscos através do desenvolvimento de software. O escopo do projeto é limitado pelos objetivos de controle obtidos diretamente da norma ISO 27001: 2013. O projeto está estruturado em fases: apresenta-se o problema em que se destacam os percalços vivenciados atualmente pelas instituições de ensino que não dispõem de SGSI, os objetivos do SICSI a desenvolver, o quadro de referência a ser desenvolvido. onde foi possível mensurar as dimensões do projeto e da solução tecnológica proposta, o quadro teórico e de referência a partir do qual foi possível mensurar as dimensões do projeto para desenvolvê-lo e implementá-lo em uma instituição de ensino. A contribuição é uma aplicação informática com o objetivo de prevenir vulnerabilidades e ameaças à qualidade do sistema de segurança. Os diferentes riscos que são causados por diferentes práticas dentro das instituições de ensino e o tratamento de cada uma podem ser identificados a fim de minimizar o impacto negativo nas mesmas. A informação das variáveis foi recolhida e analisada, documentando os resultados, gerando uma proposta para outras Universidades em situação semelhante.

Palavras-chave: Aplicativo para computador, iso 27001, instituições de ensino.

[1] Dr., Universidad Autónoma del Estado de México, jart2005@gmail.com

[2] Dra., Universidad Autónoma del Estado de México, srv_cm@hotmail.com

[3] Dr., Universidad Autónoma del Estado de México, ceeg1971@gmail.com

THE QUALITY OF INFORMATION IN A SECURITY MANAGEMENT SYSTEM (ISMS) THROUGH A SOFTWARE BASED ON THE ISO 27001 STANDARD FOR EDUCATIONAL INSTITUTIONS, MEXICO, 2021

ABSTRACT

The objective of this research was to create a computer application to improve the quality of information applied to educational institutions based on the ISO 27001 standard. It aims to reduce computer risks and proposes a risk treatment plan by developing software. The scope of the project is limited by the control objectives obtained directly from the ISO 27001: 2013 standard. The project is structured in phases: the problem is presented in which the drawbacks currently experienced by educational institutions that do not have an ISMS in place, the objectives of the SICSI to be developed, the framework of reference to be developed, are highlighted. From which it was possible to measure the dimensions of the project and the proposed technological solution, the theoretical and reference framework from which it was possible to measure the dimensions of the project to develop and implement it in an educational institution. The contribution is a computer application with the aim of preventing vulnerabilities and threats to the quality of the security system. The different risks that are caused by different practices within educational institutions and the treatment of each one can be identified in order to minimize the negative impact within them. The information of the variables was collected and analyzed, documenting the results, generating a proposal for other Universities in similar situations.

Keywords: Computer application, iso 27001, educational institutions.

INTRODUÇÃO

Hoje em dia está cada vez mais fácil que todas as informações eletrônicas de uma organização sejam roubadas ou modificadas por múltiplos indivíduos, ou mesmo por organizações que têm o objetivo de levar todas as informações possíveis para seu próprio benefício. Para isso, políticas de segurança da informação são constantemente criadas para prevenir futuros e possíveis roubos de informações. Pensar nas diferentes maneiras de escapar ou que existe uma oportunidade para roubo. Com o aumento do uso da Internet, cada vez mais empresas permitem que seus usuários, parceiros e fornecedores acessem seus sistemas de informação. Portanto, é necessário saber quais recursos da empresa precisam de proteção para controlar o acesso ao sistema e os direitos dos usuários do sistema de informação. Além disso, devido à tendência crescente para um estilo de vida nômade hoje, que permite que as pessoas se conectem aos sistemas de informação de quase qualquer lugar, elas são convidadas a fazer parte do sistema de informação com elas fora da infraestrutura segura da Organização.

Atualmente, os ataques e ameaças à segurança da informação em instituições de ensino não levam muito a sério o risco de manter todas essas informações desprotegidas e não possuem as políticas de segurança recomendadas pelas normas internacionais. Pressupõe-se que grande parte das instituições de ensino em seus departamentos de TI não possui ferramentas que auxiliem os responsáveis por essas áreas a proteger as informações depositadas nos Sistemas de Informação,

portanto, acredita-se que faltam conhecimentos tecnológicos para proteger. informações de ameaças e ataques de fatores internos e externos.

A dinâmica social e o crescimento tecnológico têm permitido às instituições de ensino aplicar os meios e recursos de que dispõem para dispor de sistemas de informação atempados, que permitam definir indicadores escolares, agilizar processos, desenhar e acompanhar o grau de avanço das linhas de ação, métodos, técnicas e estratégias, usar recursos de forma eficiente e observar as mudanças que enfrentamos em nosso ambiente para a tomada de decisão adequada. Para todos os envolvidos na Instituição, é necessário ter em consideração as informações acima descritas, de forma a ter elementos de julgamento que permitam sustentar ou modificar uma proposta de plano de ação e que permitam cumprir a missão, visão e objetivos estabelecidos na própria instituição.

É necessário saber a importância de haver qualidade no sistema de informação na gestão da educação para gerar dados confiáveis, válidos, oportunos e precisos que permitam subsidiar a tomada de decisão, por isso é uma necessidade no contexto da educação atual destacar a utilidade das ferramentas informáticas e da sua implementação nas escolas porque permite optimizar elementos e recursos, realizando de forma atempada, de forma e de forma mais produtiva e eficiente uma tarefa que exige tempo, elevados custos e esforço físico e mental.

Torna-se necessário para aquelas instituições, nas quais obviamente esqueceram a importância da administração de recursos humanos, resolver o problema que enfrentam implementando um sistema de informação sobre a dinâmica de uso dos recursos educacionais com os alunos. O cuidado com os recursos é fundamental, sua alocação deve ser ótima e cuidadosa e o controle operacional do processo deve estar a cargo de pessoas comprometidas com a capacidade de resolver o problema. Se considerarmos a entidade educacional como uma estrutura devidamente organizada, na qual a tomada de decisões é aplicada em larga escala, nas diferentes áreas dentro dela; Torna-se prioritário identificar os requisitos que os sistemas de informação devem ter na gestão da educação, uma vez que cada área atua de forma diferente, então o nível de atenção irá variar dependendo das análises feitas a partir das informações conhecidas.

Portanto, a questão da qualidade em segurança da informação para instituições de ensino é apresentada aqui. Atualmente existem vários riscos em que as informações podem ser perdidas ou extraídas sem as medidas de segurança necessárias que afetam as instituições, no entanto, isso pode ser porque não existem controles suficientes para atender a essas necessidades ou eles não são realizados. Políticas, procedimentos e controles são propostos mais especificamente para evitar a perda de informações, bem como um bom backup e proteção dos dados, pois hoje é muito importante coletar informações e também fazer um bom uso delas, pois a segurança em redes e sistemas não é um jogo porque para ter certeza em primeiro lugar, deve ser confidencial, ter pessoas competentes além de realizar vários controles que justamente nos ajudam a manter nossos bancos de dados e redes seguras, além disso, manter nossos dados atualizados. software e hardware,

também como evitar a perda de dados, o roubo de informações sensíveis e confidenciais ou a divulgação de dados do usuário que podem causar sérios prejuízos, tanto financeiros como de credibilidade.

Esta pesquisa parte da identificação de riscos, ameaças ou vulnerabilidades na qualidade da segurança da informação a que uma instituição de ensino está exposta e que são causados por diversas situações dentro dessas instituições, propondo medidas e controles, com o objetivo de manter a integridade, confidencialidade e disponibilização das informações para uma atuação positiva na Instituição. Atualmente, as informações que as organizações possuem e geram são de vital importância e transcendência, na maioria das Organizações, senão em todas, até contratos de confidencialidade são firmados onde funcionários ou ex-funcionários não podem falar sobre tais informações. Portanto, é necessário que as organizações tenham controle adequado sobre as informações e também sejam capazes de controlar o manuseio das informações pelos colaboradores.

Esta aplicação informática destina-se a pessoas ligadas às tecnologias de informação de uma instituição de ensino, quer pela responsabilidade que lhes é atribuída em relação aos ativos informáticos, quer pelos benefícios que deles obtêm. Além disso, é voltado para organizações que precisam ter o cuidado de proteger suas informações, a fim de oferecer-lhes uma proposta de como evitar qualquer risco de ataques dentro da instituição.

QUADRO TEÓRICO

Qualidade da informação.

A garantia da qualidade começa com as ações que são realizadas durante o planejamento como o conjunto de procedimentos, técnicas e ferramentas durante o ciclo de vida, atividades de auditoria como revisões técnicas ou inspeções, otimizando os critérios previamente definidos e as funções da informação de gestão, mais orientada para documentação e desenvolvimento de testes.

Os sistemas de informação permitem medir o valor, reconhecer os pontos fortes e fracos de uma escola, compará-la com outras escolas, identificar indicadores comuns que a medem com elevado grau de fiabilidade, que podem ser lidos e interpretados com base no grau de desenvolvimento e evolução de sistemas e instituições. A qualidade da segurança da informação é o conjunto de medidas técnicas, operacionais, organizacionais e legais que permitem às organizações salvaguardar e proteger as informações. O conceito de segurança da informação não deve ser confundido com o de segurança informática, uma vez que este último trata apenas da segurança no meio informático, mas as informações podem ser encontradas em diferentes suportes ou formas, e não apenas nos suportes informáticos. A qualidade da segurança da informação (Wendy, Wang, 2019) é responsável por garantir a: Integridade: propriedade de salvaguardar a exatidão e o estado completo dos ativos de informação, Disponibilidade: propriedade da informação ser acessível e utilizável por solicitação de uma entidade autorizada, e Confidencialidade: propriedade que determina

que a informação não está disponível ou divulgada a pessoas, entidades ou processos não autorizados.

Atualmente, as empresas têm experimentado um alto crescimento no vazamento de informações, onde documentos confidenciais são expostos fora da empresa. O maior desafio para controlar o vazamento de informações nas empresas são os funcionários, uma vez que, voluntária ou involuntariamente, eles causam o vazamento de informações. Isso cria uma imagem ruim ou reputação corporativa, uma vez que a incapacidade de controlar ataques ou vazamento de informações críticas é questionável. A gestão da segurança da informação é uma questão importante para garantir a integridade das informações nos sistemas. Esses padrões se concentram em um conjunto de vulnerabilidades ou riscos, internos e externos, que devem ser tratados por meio da aplicação de um conjunto associado de controles. Esses controles são salvaguardas físicas ou administrativas sugeridas nas normas, com o objetivo de evitar ou mitigar riscos.

Atualmente, nas diferentes organizações que enfrentam uma concorrência de classe mundial, a qualidade passa a ser um importante diferencial, além de aumentar a satisfação geral do cliente, reduzindo custos e otimizando recursos. Os produtos ou serviços com certificados de qualidade são preferidos pelos compradores porque transmitem segurança e confiança. Este também é um atributo valioso para estratégias de marketing no exterior. O conceito de qualidade total visa buscar a excelência em tudo o que o homem, a sociedade e as organizações fazem. Este conceito também se aplica ao desenvolvimento de sistemas de informação baseados em equipamentos de processamento de informação e programas feitos pelo homem.

Software existente.

O Software ISOTools Excellence para ISO / IEC 27001: 2013 para o Sistema de Gestão da Segurança da Informação ou SGSI é composto por diversos aplicativos que, quando reunidos, trabalham para que as informações tratadas pelas Organizações não percam nenhuma de suas propriedades. Importante: disponibilidade , integridade e confidencialidade. Em um cenário de desenvolvimento de software interno, uma organização que alega ser certificada ou mantém uma certificação deve cuidar de certos aspectos do desenvolvimento de software.

Um padrão IS (Tofan, 2019) é estruturado por um conjunto de controles agrupados em domínios. A principal referência para os padrões IS, ISO 27001 (Gilliam, 2009), é reconhecida como o padrão mais difundido em todo o mundo (Buecker, 2019). Outros modelos comumente citados e também com uma cobertura mais ampla do que apenas segurança são os padrões ITIL (Official ITIL) e COBIT (ISACA)].

A gestão da segurança da informação deve atender a um objetivo claro: reduzir o nível de risco a que a instituição de ensino está exposta. Ter segurança adequada nos sistemas de gestão da informação nas instituições de ensino é de grande importância, pois, evita qualquer hacking e perda de

informações de critérios valiosos, para melhor implementar o SGSI é importante manter um controle e é aí que entram as auditorias, onde eles revisam o que está sendo feito bem e mal e para isso aplicar melhorias e / ou mudanças dentro da parte de informática da instituição. O acesso não autorizado a sistemas e infraestruturas é outro dos principais riscos a evitar. Grande parte desse acesso não autorizado poderia ser evitado se os sistemas e aplicativos fossem atualizados adequadamente. A atualização é considerada parte fundamental de uma boa gestão e responsabilidade corporativa, pois proporciona maior segurança e denota um trabalho de melhoria contínua que beneficia a aplicação e o usuário.

As organizações devem adotar uma abordagem proativa para identificar e proteger todos os seus ativos mais importantes. O estabelecimento de um plano de tratamento de riscos de segurança da informação permite à Organização avaliar o que deseja proteger e utilizá-lo como elemento de apoio para tomar a decisão de identificar diferentes medidas de segurança. A avaliação abrangente dos riscos de segurança da informação permite que uma organização avalie os riscos potenciais no contexto de suas necessidades. É muito importante ter em mente que o propósito dos sistemas de informação e dos dados que eles contêm é apoiar os processos da Organização, que por sua vez apóiam a missão da Organização. A informação é um elemento fundamental que contribui para a capacidade da Organização de sustentar suas operações.

Para realizar a implantação da norma ISO 27000, a utilização de um programa específico de gestão de riscos é uma excelente opção que permite, por um lado, economias consideráveis de custos e tempo e, por outro, a capacidade de realizar um controle exaustivo de todas as fases do processo, bem como dos resultados e da identificação de possíveis pontos de melhoria e riscos para a empresa. Ao implementar e certificar a norma ISO 2700, para o SGSI (Sistema de Gestão de Segurança da Informação) da organização, pode-se demonstrar de forma particular que a entidade atende a todos os requisitos mínimos para garantir a segurança da informação.

As organizações devem ter um modelo ou sistema de gestão de segurança da informação baseado em padrões de segurança mundialmente reconhecidos, a fim de estabelecer e manter a segurança alinhada às necessidades e objetivos estratégicos da organização, composta por uma estrutura organizacional, com papéis e responsabilidades e um conjunto coerente de políticas, controles, processos e procedimentos, que permitem gerenciar adequadamente os riscos que possam ameaçar a confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e irrecusabilidade da segurança da informação.

Para alcançar uma qualidade de informação adequada, é imprescindível que as organizações estabeleçam uma metodologia estruturada, clara e rigorosa de avaliação e tratamento dos riscos de segurança, com o objetivo de: conhecer o estado real da segurança dos ativos de informação através dos quais os negócios a informação é gerenciada, identificar e avaliar ameaças que possam comprometer a segurança da informação e determinar os mecanismos e medidas de segurança a

serem implementados para minimizar o impacto em caso de possíveis perdas de confiabilidade, integridade e disponibilidade das informações.

As organizações lidam com grandes volumes de dados de terceiros que devem ser tratados de acordo com os requisitos da legislação, garantindo aos clientes a segurança de suas informações nos mais elevados padrões de qualidade relacionados à segurança da informação. As tecnologias e as comunicações ganham cada vez mais importância nas organizações pelo apoio que prestam à sistematização e organização da informação. No entanto, devido a diversas vulnerabilidades e ameaças, os Sistemas de Informação podem colocar em risco a integridade, confidencialidade e disponibilidade da qualidade da informação, para os quais os riscos devem ser geridos de forma a minimizar os danos à organização através da prevenção e redução do impacto de incidentes de segurança. Atualmente, a maioria das empresas que implementam o ISMS usa ferramentas como planilhas para realizar análises de GAP para determinar o grau de conformidade com os requisitos estabelecidos no padrão NTC-ISO-IEC-27001.

A implementação de um SGSI permite à organização realizar uma análise de risco; identificação de ameaças, vulnerabilidades e impactos na atividade organizacional, melhoria contínua na gestão da segurança, garantia da continuidade e disponibilidade do negócio, redução de custos relacionados a incidentes, aumento dos níveis de confiança do cliente, aumento da comercialização de valor e melhoria da imagem da organização, atendimento aos atuais legislação sobre protecção de dados pessoais, serviços da sociedade da informação, comércio electrónico, propriedade intelectual e em geral, a relativa à segurança da informação. Esta implementação da qualidade da informação através de uma ferramenta de software acompanhada de técnicas de Visualização de Dados, facilita a interpretação das informações e a tomada de decisões para a gestão dos sistemas de qualidade em segurança da informação. Para desenvolver esta aplicação informática foi necessário conhecer os conceitos técnicos e jurídicos que se relacionam diretamente com a matéria e ter um suporte teórico e jurídico que permita esclarecer definições de forma a responder aos requisitos do projeto. Hoje em dia as empresas e as pessoas tendem a sistematizar as tarefas que realizam de forma repetitiva para otimizar o tempo e tomar decisões de forma inteligente, por isso sistemas de gestão não são alheios a esta situação e devem ser implementadas ferramentas informáticas que permitam a análise dos dados e fácil compreensão por parte dos utilizadores. níveis. Para realizar uma análise simples, é fácil encontrar modelos no Excel que permitem estes diagnósticos de forma fácil, razão pela qual é feito um aplicativo de computador que facilita este processo.

Normas ISO 27001: 2013.

Este padrão é o padrão internacional para gerenciamento de segurança da informação. Define como implementar um sistema de gerenciamento de segurança da informação avaliado e certificado de forma independente. Isso permite que você proteja com mais eficiência todas as informações financeiras e confidenciais de uma forma que reduza a possibilidade de serem acessadas ilegalmente ou sem autorização. Com a ISO / IEC 27001: 2013, o comprometimento e a

conformidade com as melhores práticas globais podem ser demonstrados, demonstrando aos clientes, fornecedores e partes interessadas que a segurança é essencial para a forma como a Organização opera.

A norma ISO / IEC 27001: 2005 é uma norma reconhecida internacionalmente, que especifica os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI), considerando os riscos do negócio (ISO 27000 Oficial) Em outras palavras, propõe uma metodologia para implementar a ISO, especificando os requisitos para a aplicação de controles de segurança a um SGSI. Este padrão segmenta a segurança em onze domínios e propõe um conjunto de controles dentro deles.

A maioria das organizações baseia suas operações em sistemas de computador. Esta situação se manifesta através dos padrões IS, que apresentam o problema de segurança como um conjunto de controles que representam garantias para as diferentes vulnerabilidades de segurança. Por outro lado, deve-se considerar que também existem regulamentações nacionais que não necessariamente se alinham aos padrões internacionais, o que significa que a organização deve cumprir ambos os requisitos. Isso é ainda mais agravado, se for considerada uma organização governamental, que também deve cumprir as regulamentações governamentais internas. Isso coloca a organização em apuros quanto a qual padrão aplicar ou que nível de conformidade deve ser alcançado com os padrões que está interessada em atingir.

Diante dessa situação, a incorporação de novos sistemas dentro de uma organização que seja certificada de acordo com uma norma ou em vias de fazê-lo, é uma decisão importante, pois a incorporação de sistemas que não estejam em conformidade com a norma pode levar a perder a certificação. Este fenômeno nos obriga a considerar os efeitos ou requisitos dos padrões no desenvolvimento de novos sistemas, portanto, os controles estabelecidos nos padrões têm impacto nas diferentes etapas do desenvolvimento do Software.

A ISO (International Standardization Organization) é o órgão encarregado de promover o desenvolvimento de padrões internacionais de fabricação, comércio e comunicação para todos os ramos industriais. A principal função é buscar a padronização de padrões de produtos e segurança para negócios, empresas e organizações em nível internacional. As normas criadas pela ISO são voluntárias, não têm autoridade para impor suas normas a nenhum país, uma vez que a ISO é uma entidade não governamental e não depende de nenhuma outra entidade internacional. A Norma ISO 27000 é uma norma internacional e aberta, cujo objetivo é estabelecer uma série de requisitos mínimos que um Sistema de Gestão de Segurança da Informação (SGSI) deve atender em uma organização, pública ou privada, grande ou pequena. As empresas procuram meios eficientes que lhes permitam garantir e gerir a segurança das informações e os meios que as processam. A série ISO 27000 é aquela que reúne todas as normas de segurança da informação, sendo as mais importantes as normas ISO 27001 e ISO 27002.

A principal diferença entre esses dois padrões é que o 27001 é baseado no gerenciamento contínuo da segurança, apoiado na identificação dos riscos ao longo do tempo. É um padrão que as organizações devem certificar. Ele contém uma série de requisitos que uma organização deve atender para estar de acordo com as boas práticas. Hoje é a certificação de segurança mais popular e é aplicada por empresas de todos os tipos em um nível universal. O padrão 27002 é um guia de boas práticas que descreve uma sucessão de objetivos de controle e gerenciamento que devem ser recomendados para fornecer segurança na organização. É um padrão não certificável. O padrão ISO 27003 fornece instruções sobre como abordar o planejamento de gestão para implementar o SGSI. O padrão ISO 27004 fornece uma série de melhores práticas para medir o resultado de um SGSI. O padrão ISO 27005 contém várias recomendações e diretrizes gerais para o gerenciamento de riscos de segurança da informação. A norma ISO 27006 responde a um guia para organismos de certificação nos processos formais que devem ser seguidos durante a auditoria de SGSI. O padrão ISO 27007 é um guia para auditar o SGSI. O padrão ISO 27799 é um guia a ser implementado no setor de saúde. O padrão ISO 27035 fornece uma abordagem de prática recomendada para gerenciar informações de incidentes de segurança para organizações.

As normas permitem que as organizações apresentem e certifiquem um nível de qualidade para o público em geral, demonstrando que possuem os controles e técnicas adequados para garantir o tratamento dos dados e informações com que são tratados. No início foram considerados de grande interesse para grandes empresas, e atualmente as normas ISO 27000 estão sendo estudadas por empresas de médio porte em todo o mundo. Esta norma é aplicável a qualquer organização que possua sistemas de informação. Cumprindo as normas legais de proteção de dados, é possível reduzir os problemas com clientes e usuários. Oferece garantia de continuidade dos negócios com base no Plano de Contingência. Aumentar o valor comercial da empresa e parceiros; bem como uma grande melhoria na imagem da organização. Aumento dos níveis de confiança de fornecedores, clientes, acionistas e parceiros.

Os Sistemas de Gestão de Segurança da Informação de acordo com a norma ISO / IEC 27001: 2013 devem ser continuamente aprimorados seguindo a filosofia, aplicando a metodologia de ciclo PDCA (Planejar, Fazer, Verificar e Agir), (Aldya: 2019) isso é feito quando software, hardware, etc. são atualizados. Um sistema de gestão de segurança informática (SGSI) garante a confidencialidade, integração e disponibilidade dos dados.

MÉTODO

O projeto é desenvolvido com uma abordagem quantitativa, onde serão quantificadas as diferentes propriedades das variáveis envolvidas no projeto. É uma pesquisa descritiva porque mede as variáveis para gerar os dados. A pesquisa é não experimental e transversal, as variáveis são estudadas em um tempo definido, onde foi determinada a forma mais adequada de mensurar esse

conjunto de variáveis para poder dar uma visão geral do estado dos controles de segurança da informação e se atendem a ISO / IEC 27001 de 2013 e respeitam a qualidade das informações.

Para a criação do software do Sistema de Gestão da Qualidade da Segurança da Informação (SGCSI) e mensuração do modelo de maturidade, foi levado em consideração:

Análise de lacunas (GAP) na ISO 27001.

Uma análise de lacunas (GAP) é um método de avaliação das diferenças de desempenho entre os sistemas de informação ou aplicativos de software de uma empresa para determinar se os requisitos de negócios estão sendo atendidos e, se não, quais etapas devem ser executadas para garantir que sejam atendidos com êxito. A lacuna se refere ao espaço entre "onde estamos" (agora) e "onde queremos estar" (a meta a ser alcançada). Uma análise de lacunas também pode ser chamada de análise de necessidades, permitindo-nos determinar o que está faltando e os recursos necessários para atingir nossos objetivos.

Uma análise de lacunas (GAP) ou análise de deficiência, portanto, consiste em uma análise de conformidade com os requisitos da ISO 27001 e seus controles. Portanto, é algo semelhante a uma auditoria inicial semelhante às melhores práticas de auditoria em uma organização (Amogh Phirke, 2019), então você pode ter uma ideia do grau de implementação da norma ISO 27001 na organização pode servir a um objetivo duplo. Estabelecer o ponto de partida para implementar a norma e avaliar o esforço necessário, bem como ter uma ferramenta confiável para desenvolver um plano de implantação da ISO 27001, também manter uma ferramenta para avaliar o grau de implantação da norma durante o processo de implantação e avaliar o grau de andamento do projeto

Análise de risco vs análise de lacunas.

Uma análise de conformidade com os requisitos e controles da ISO 27001 não deve ser confundida com uma análise de risco. A análise de conformidade identifica quais requisitos e controles incluídos no padrão implementamos na organização e em que grau. Por outro lado, uma análise de risco oferece como resultado os controles de segurança da informação que realmente precisam ser implementados. Em outras palavras, uma análise de risco estabelece a justificativa para os controles que devem ser implementados para a segurança da informação.

Dependendo do tamanho e escopo do projeto, uma análise de lacunas pode ser realizada antes de iniciar a implementação da norma para avaliar a situação inicial e planejar os recursos necessários para o projeto. Anteriormente, o padrão de análise GAP era útil na preparação da declaração de aplicabilidade. Porém, na versão atual da ISO 27001: 2013 é necessário realizar previamente uma análise de risco para determinar o real escopo dos controles a serem implementados.

Para obter um relatório de auditoria inicial sobre a conformidade com a norma, uma lacuna de GAP ou análise de deficiência pode ser realizada antes de iniciar o projeto aplicado aos requisitos

genéricos da norma. Com base na análise de risco, é possível, por meio da análise da conformidade dos controles, obter o relatório para estabelecer o plano de sua aplicação e seu status de conformidade, além de nos auxiliar na elaboração da Declaração de Aplicabilidade.

Para a realização da análise de deficiência de GAP em segurança da informação, pode ser aconselhável a utilização de um modelo de maturidade para avaliação de conformidade. Os modelos de maturidade mais comuns como NIST, CITI-ISEM, COBOT, SSE / CM e CERT / CSO propõem um modelo de 5 a 6 níveis de maturidade ou conformidade. Esses modelos de maturidade comumente usados como ferramentas para gerenciamento de serviços de TI são usados para avaliar o desempenho dos processos de gerenciamento em relação aos controles internos. Este modelo é adaptado para estabelecer um modelo de auditoria que nos permite medir seu atual nível de maturidade em relação aos requisitos de uma norma específica, neste caso ISO27001.

Com isso, a análise de deficiência de GAP revelará as melhores práticas para os controles internos do sistema de Gestão da Segurança da Informação. Os níveis de maturidade não são um objetivo, mas sim um meio de avaliar a adequação dos controles internos aos objetivos do sistema de gestão.

Entre as vantagens de realizar uma análise de deficiência usando um modelo de nível de maturidade estão as seguintes:
1. Fornece um modelo para um programa de segurança completo.
2. Fornece informações adequadas aos gerentes para implementar controles de segurança.
3. Orienta para o uso de padrões de melhores práticas (ISO 27001).

Nesse modelo, podem ser avaliados tanto a existência ou inexistência quanto o grau de implementação dos 11 controles (domínios) que compõem a ISO27001. Para o desenvolvimento da aplicação no seu relatório de gestão foram considerados os seguintes 6 níveis de maturidade:

(Nível 0), Inexistência: não há reconhecimento da necessidade do controle ou requisito.
(Nível 1), Ad-hoc: Há algum reconhecimento da necessidade de controle interno ou requisito. É aplicado para um problema ou tarefa específica, não generalizável.
(Nível 2), Executado - os controles existem, mas não são documentados.
(Nível 3), Definido - os controles estão implantados e adequadamente documentados.
(Nível 4), Manipulável e mensurável: Existe controle interno sobre a aplicação dos controles e o cumprimento do requisito.
(Nível 5), Otimizado: Há controle interno e contínuo sobre a aplicação dos controles e o cumprimento dos requisitos. A eficácia dos controles é medida pelo estabelecimento de objetivos de melhoria.

Para tal, utilizou-se uma lista de questões para obter o grau de conformidade da organização em diferentes cenários de acordo com os níveis de maturidade definidos. Isso permite definir um nível de

maturidade para cada um dos 11 controles. Isso foi resolvido desenvolvendo as questões usadas nos controles da norma ISO 27001 para obter seus valores de maturidade.

Critérios de avaliação.

Se eles atribuíram valores de acordo com os níveis de maturidade de 0 a 5 para cada controle, obtendo para cada controle um nível médio de maturidade que será determinado por:

Conformidade de nível médio = pontuação total de cada controle / número de controles totais

Esta fórmula entregará um valor médio para cada controle entre 0 e 5, de forma que os controles e sua conformidade possam ser classificados entre os seguintes valores:

Pontuação de maturidade abaixo de 1,65: Não cumpre
Pontuação de maturidade entre 1,66 e 3,25: parcialmente compatível
Pontuação de maturidade acima de 3,26: Conformidade com os requisitos da Norma

Tudo isso influenciou o desenvolvimento de um software para medir a qualidade da Segurança da Informação em uma Organização e saber se ela atende aos níveis de maturidade exigidos pela Norma ISO 27001.

RESULTADOS

Desenvolvimento da aplicação informática.

O software elaborado permite o estabelecimento de medidas de segurança da informação em qualquer tipo de organização. Para isso, possui um sistema modular que permite a entrada de informações por meio da colaboração de gestores, gerentes de área e equipe de apoio. Recebe feedback das informações e permite ao responsável pela segurança da informação realizar uma análise e obter relatórios imediatos que, ao serem analisados pelos Gestores, permitirão tomar as medidas adequadas para minimizar os riscos a que estão expostos os ativos críticos da organização , em seus diferentes aspectos na segurança da informação. Os gerentes seniores perceberam que a informação é um recurso crítico e talvez o mais importante na organização e, por esse motivo, deve ser tratada de forma adequada como qualquer outro ativo na organização.

A segurança da informação é baseada na disponibilidade, integridade e confidencialidade dos ativos de informação. Existe um manual que fornece a lógica com que o software foi desenhado e seus componentes tecnológicos sobre os quais funciona corretamente, bem como sua correta instalação. No aplicativo de computador que foi desenvolvido, fotos, vídeos, documentos e notas podem ser carregados por USB ou pelo celular. Os documentos que podem ser obtidos são: Políticas, Medidas, Procedimentos, Controles, Riscos, Sugestões, Livro contendo informações sobre cada ponto da Norma ISO 27001 para esclarecer mais detalhadamente as dúvidas a respeito. Documentos podem ser cadastrados para uma eventual auditoria, cada um dos pontos de controle da Norma ISO 27001

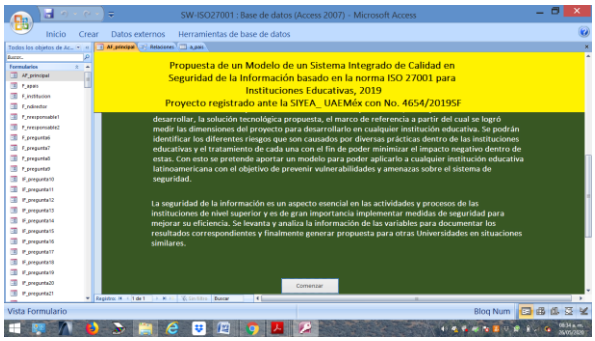
pode ser impresso separadamente, acordos podem ser assinados e salvos através da união do aplicativo Adobe Reader, podem ser enviados documentos por e-mail para cada um dos pontos da Norma, você pode ter relatórios sobre prestadores de serviço, você pode obter relatórios para a Gestão da Instituição, você pode obter relatórios de acompanhamento faltantes para cada ponto da Norma, as diferentes análises e relatórios permitem decisões oportunas para a diferentes pessoas envolvidas.

O desenho da base de dados é realizado levando-se em consideração a estrutura de controles prevista na norma ISO-IEC-27001: 2013. Esta aplicação informática foi desenvolvida para as informações solicitadas na ISO 27001. É uma aplicação para que cada utilizador possa captar as suas informações relacionadas com as questões do questionário para instituições de ensino com a ISO 27001 e também permite visualizar sugestões.

Começa com uma tela onde diz aviso de segurança, a seguir clique em AF_principal e apresenta uma introdução, após ter lido, clique no botão: Iniciar. (Veja a Figura 1). Nesse desenvolvimento, as respostas das instituições públicas e privadas foram tomadas como base para que as respostas obtidas pudessem ser tomadas como exemplo. (Aqui os nomes das instituições e dos responsáveis foram apagados intencionalmente). Em cada questão é possível ver sugestões de Políticas, Medidas, Controles e Procedimentos (Ver Figura 3). Para sair das sugestões, clique em voltar à pesquisa para continuar capturando as informações relacionadas à Instituição. Continua com as 151 questões (Ver Figura 2) e por fim na sugestão 151 você também pode ver um livro com o referencial teórico sobre o conteúdo da Norma ISO 27001 (Ver Figura 4), para complementar todas as informações, referências bibliográficas, glossário bem como consultar os créditos dos autores e dos assistentes de pesquisa envolvidos. Para sair do aplicativo, clique em finalizar captura. Você também tem a opção de imprimir as informações capturadas em detalhes para cada item ou em resumo.

Figura 1

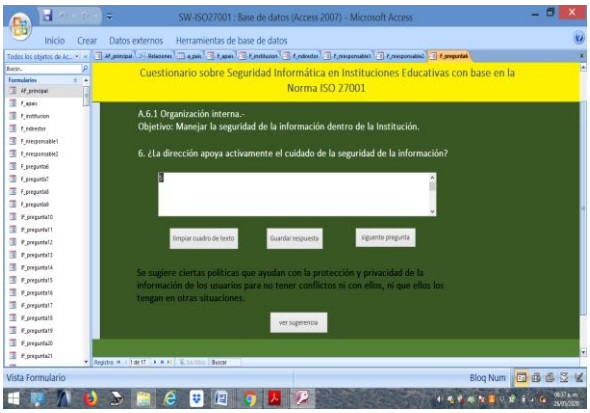
Tela inicial do aplicativo de computador



Fonte: self made.

Figura 2

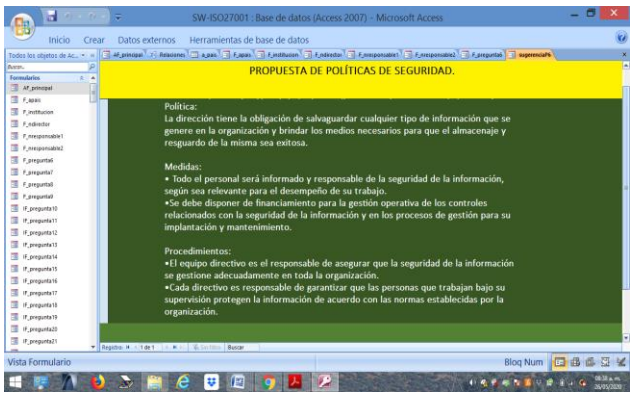
Exemplo de perguntas do questionário de 151 itens.



Fonte: self made.

Figura 3

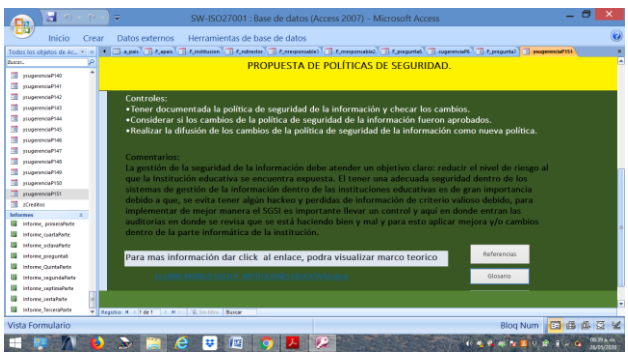
Exemplo de políticas, medidas, controles e procedimentos em cada uma das questões.



Fonte: self made.

Figura 4

Exemplo de proposta de revisão do link do livro contendo também o referencial teórico sobre o conteúdo da Norma ISO 27001.



Fonte: self made.

Foi desenvolvida a construção de um referencial teórico, que parte da qualidade da segurança da informação aos padrões a serem estudados e aos requisitos da ferramenta a ser desenvolvida. Foram aplicados e desenhados formatos de técnicas de coleta de informações: análise de conteúdo e observação não estruturada; A análise dos resultados delimitou o projeto no sentido da implementação de etapas fundamentais para o processo de desenvolvimento e implementação do SGSI. Procedeu-se à seleção de padrões internacionais de qualidade para a segurança da informação, identificando-se aspectos comuns que os caracterizam e permitem descrever as suas finalidades e forma de trabalho. Desta forma, vantagens e desvantagens eram conhecidas. A seção de desenvolvimento da metodologia corresponde à descrição das estratégias técnicas e teóricas aplicáveis ao esquema requerido para o desenvolvimento do software. Com a teoria, estabeleceu-se a definição da metodologia a ser aplicada na seleção das características e elementos componentes do modelo de software, passando da teoria à prática (Ionna Topa, 2019). Foi desenhada a arquitetura de software que corresponde à implementação do modelo de software.

Relatórios de SW.

Os relatórios disponibilizados ao software são: Planejamento do Projeto, Documento de escopo do SGCSI, Diagnóstico Inicial, Diagnóstico Quantitativo do SGCSI, Política de Segurança da Informação, Políticas de Segurança da Informação, Funções e Responsabilidades, Gestão de Risco de SGCSI, Software de Tratamento de Risco (Desenvolvimento próprio para gerenciar riscos), Documentação, SGCSI Gestão de Riscos, Tratamento de Riscos (Desenvolvimento próprio para gerenciar riscos), Relatórios de auditoria para revisão pela Administração. O relatório de estatísticas apresenta uma visão abrangente da Organização, mostrando a situação da segurança da informação para cada um dos pontos de controle ou, se preferir, um relatório específico sobre algum dos objetivos de controle em particular.

CONCLUSÕES

O processo de implementação do software implica comprometimento por parte de toda a organização, portanto, se apenas o departamento de TIC estiver envolvido, isso não leva ao sucesso da implementação do SGSI. É necessário que as funções e tarefas correspondentes sejam atribuídas a cada um dos envolvidos na organização. Cada uma das pessoas deve estar ligada para participar ativamente no desenvolvimento da qualidade do sistema de segurança, pois de uma forma ou de outra a informação é acessível a todos os envolvidos. O empenho total na hora de implementar um SGSI deve ter o seu conhecimento por parte dos gestores, de forma a minimizar a dependência e a forma de ver este processo como uma responsabilidade não só do departamento de TIC.

É necessário conhecer os riscos a que a organização está exposta e através de uma análise estabelecer o tratamento que se considera mais adequado. Algumas organizações descrevem uma "análise de risco", onde avaliam apenas subjetivamente algumas ameaças sobre os ativos que melhor conhecem, sem ter uma ideia clara de seu valor e, por outro lado, sem constituir a totalidade

dos ativos da organização. Saber o que pode acontecer e as consequências que esse evento geraria são aspectos fundamentais na definição de uma boa estratégia de segurança.

A análise das variáveis propostas permitiu uma melhor estruturação do software, bem como a forma mais adequada de definir as ideias que se tinham para a programação do referido software. Foi levantada a possibilidade de designar gestores da instituição de ensino para inserir apenas as informações adequadas ao software quanto às funções dos envolvidos. Depois de analisar as várias situações que podem surgir ao inserir a informação no software, o esquema de utilização foi levantado com o gestor de TIC pelo seu conhecimento e experiência que lhe dá valor acrescentado, a fim de ser um suporte e ajudar a captar os dados solicitados no termos de segurança da informação, obtendo-se assim a criação de subsídios no software para inserir apenas as informações solicitadas e obter bons resultados nos relatórios finais.

Portanto, conclui-se que o desenvolvimento do software atende às expectativas de funcionalidade e parametrização da qualidade em segurança da informação, pois foi formulado sob os parâmetros da norma ISO 27001: 2013. Este desenvolvimento de software obedece à realização de uma análise da qualidade da segurança da informação, sendo esta a base para o estabelecimento de um SGSI nesta Instituição de ensino, bem como para qualquer Organização que pretenda estabelecer medidas para a segurança da sua informação.

Os módulos de suporte apresentados no âmbito da solução deste software, foram definidos por várias investigações que, para além de confirmarem a complexidade associada à selecção e aplicação de normas, permitiram responder aos objectivos traçados, através de diferentes métodos, de segurança informática , técnicas formais de coleta de informações, análise estatística de relatórios e determinação de critérios de avaliação de padrões para a consolidação dos módulos.

O modelo de software apresentado para a implementação do SGSI é uma ferramenta que oferece análise de risco, sugestões específicas, documentação metodológica, revisão frequente, tratamento de não conformidades. No software desenvolvido foram realizadas tarefas de coleta de informações, análise de dados, compreensão e aplicação de teorias, entre outras, que permitiram a troca de conhecimentos e habilidades. O produto final constitui um software e ferramenta de facilitação e consolidação de objetivos que descreve processos de apoio ao processo de implementação do Sistema da Qualidade em medidas de Segurança da Informação.

Com a aplicação informática apresentada neste documento, são propostas diferentes estatísticas, procedimentos, políticas, tipos de controlos, medidas de segurança para o controlo da informação e os sistemas que constituem uma peça chave nas organizações para a tomada de decisões dos gestores das organizações. Você deve analisar os riscos informáticos que as organizações enfrentam atualmente, para os seguintes resultados alcançados: fornecer políticas, medidas, procedimentos e controles de uso, estatísticas, controle e salvaguarda da qualidade da segurança da

informação dois sistemas de organização no momento de implementação de uma aplicação informática do SGSI, para proteger os riscos a que estão sujeitos e ao mesmo tempo fornecer soluções que acompanham os problemas presentes e futuros que possam surgir.

REFERÊNCIAS

Aldya et al, Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard, 2019 IOP Conf. Ser.: Mater. Sci. Eng. IOP Conference Series: Materials Science and Engineering, doi:10.1088/1757-899X/550/1/012020

Amogh Phirke. (2019). Best practices of auditing in an organization using ISO 27001 standard, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S3, July 2019

Buecker, A., Borrett, M., Lorenz, C. and Powers, C. (2019). “Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security,” Report REDP-4528-01, 2019.

Gilliam, D.P.; Wolfe, T.L.; Sherif, J.S.; Bishop, M. (2020). "Software security checklist for the software life cycle," Enabling Technologies: Infrastructure for Collaborative Enterprises, 2020. WET ICE 2019, pp. 243- 248, 9-11 June 2020, doi: 10.1109/ENABL.2003.1231415

Ioanna Topa. (2020). “From theory to practice: guidelines for enhancing information security management”, Information and Computer Security, ISSN: 2056-4961, Publication date: 8 July 2019

ISACA: Control objectives for information and related technologies (COBIT),” http://www.isaca.org/Knowledge-Center/cobit/Pages/Products.aspx.

ISO 10006 (2003). Sistemas de gestión de la calidad — Directrices para la gestión de la calidad en los proyectos.

ISO 21500 (2012). Orientación sobre la gestión de proyectos.

ISO 25000 (2006). Requisitos, evaluación de la calidad del sistema y del software.

ISO 27002 http://iso27000.es/iso27002.html, https://www.isotools.org/software/riesgos-y-seguridad/iso-27001

ISO/IEC 27000 (2005). Dominios y Controles de gestión ISO 27000. Portal ISO 27000 en español. http://www.iso27000.es/download/ControlesISO27002-2005.pdf.

ISO/IEC 27000 (2013). Standard ISO 27000. Portal ISO 27000 en español. Recuperado de http://www.iso27000.es/iso27000.html.

ISO/IEC 27001:2005, “Information technology -- Security techniques -- Information security management systems -- Requirements,” Edition: 1 | Stage: 90.92 | JTC 1/SC 27 ICS: 35.040.

Norma UNE-EN ISO 27001:2005. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Project Management Institute.

Official ISO Website, http://www.iso.org/

Official ITIL Website, http://www.itil-officialsite.com/

PMBOK (2020). Guía de los Fundamentos para la Gestión de Proyectos. 5º Edición. Project Management Institute.

Tofan, D. (2019). “Information Security Standards,” Journal of Mobile, Embedded and Distributed Systems, vol. 3, pp. 128-135, 2019.

Wendy, Wang. (2019). Measuring information security and cybersecurity on private cloud computing, Journal of Theoretical and Applied Information Technology, 15th January 2019. Vol.96. No 1, ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195.