NOME:	RA:
Daniel Henrique dos Santos Rodrigues	2830972313028
Luiz Felipe Rosa moura	2830972313022
Maicon Wansley Antunes da Silva	2830972313002
Vitor Almeida da Silva	2830972313014
Yuri Gabriel Jales da Silva	2830972313021

Plano para implementação de um SGSI (sistema de gestão de segurança da informação) na fabricante de componentes industriais TechPro.

O planejamento para implementação do SGSI conforme os padrões da ISO 27001 visa garantir a segurança de quaisquer ativos de informação críticos, garantir a confidencialidade, a integridade e a disponibilidade dos dados assim atendendo as regulamentações do setor. A base do planejamento serão quatro tópicos, sendo eles: a avaliação inicial da situação; o desenvolvimento do plano de Implementação; o atendimento aos requisitos da ISO 27001 e a apresentação do plano de implementação.

A avaliação inicial da situação por sua vez ocorrerá em com base em três etapas conforme descrito abaixo

A) **Identificação dos ativos de informação críticos:** esses ativos identificados na operação da TechPro incluem projetos de engenharia (como especificações de produtos para clientes), dados de pesquisa e desenvolvimento, informações financeiras da instituição e de clientes; Informações de recursos humanos (como dados de colaboradores); Informações de perímetro; informações sobre processo fabril e métodos de produção/operação - como maquinários).

B) **Avaliação de ameaças e vulnerabilidades:** realizada com um método sugerido no curso "Gerenciamento de ameaças cibernéticas" da Cisco, esse tópico foi segregado em algumas categorias de risco, dessa forma facilitando averiguação do cenário geral:

- **Adversarial:** Observamos uma presença significativa de ameaças adversariais, incluindo ataques de phishing direcionados aos funcionários, tentativas de ransomware visando os sistemas críticos da empresa e uma exposição contínua a ataques de negação de serviço (DDoS) por parte da infraestrutura online.
- **Acidental:** Notamos uma preocupação séria com erros humanos que levam a vazamentos de dados sensíveis, como a divulgação inadvertida de informações confidenciais por colaboradores. Além disso, há uma tendência preocupante de instalação de software malicioso por descuido, o que aumenta o risco de comprometimento da segurança dos sistemas assim como o uso de unidades portáteis de armazenamento (como pen drives).
- **Estrutural:** Identificamos várias vulnerabilidades de softwares na infraestrutura, juntamente com configurações inadequadas de segurança que deixam os sistemas expostos a ameaças. Além disso, a falta de aplicação regular de patches de segurança tem sido uma área de preocupação, pois deixa os sistemas vulneráveis a explorações externas e até internas.
- **Ambiental:** Reconhecemos a possibilidade de desastres naturais, como terremotos e incêndios, representarem uma ameaça física à infraestrutura de rede. Além disso, falhas de energia recorrentes têm o potencial de interromper as operações e causar indisponibilidade dos sistemas ainda mais considerando a falta de um gerador de energia nas instalações.

C) **Identificação das regulamentações e normas aplicáveis:** Após avaliação detalhada do cenário em que se encontra a organização em que serão aplicados os procedimentos de segurança foram definidas as leis e práticas a serem seguidas para garantir o escopo de segurança proposto a nível internacional, sendo as principais:

- **LGPD (Lei Geral de Proteção de Dados Pessoais):** Promulgada para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo.
- **ITIL (Information Technology Infrastructure Library):** Modelo de referência para gerenciamento de processos de TI.
- **COBIT (Control Objectives for Information and Related Technology):** Guia de boas práticas apresentado como framework e mapas de auditoria, conjunto de ferramentas de implementação e guia com técnicas de gerenciamento.

Para o desenvolvimento do plano de Implementação foram estabelecidas outras três etapas a serem explorados, sendo elas:

A) **Estabelecimento de um comitê de segurança:** após análise da estrutura hierárquica da TechPro, ficou alinhado que o comitê de segurança da informação terá a seguinte composição.

I. Gestor de segurança da informação da ConsuTech, que o coordenará.
II. O titular de tecnologia da informação da unidade.
III. O representante da Secretaria-Executiva da unidade.
IV. Os representantes de cada um dos setores críticos da unidade (pesquisa e desenvolvimento, financeiro, recursos humanos, supply chain, jurídico e operacional).

B) **Definição de escopo e limites do SGSI:** a ConsuTech pretende se responsabilizar por todo o planejamento para a implementação do SGSI, entretanto, ficará responsável apenas pela segurança lógica do cliente e o treinamento dos funcionários. É necessária também a conformidade e segurança da rede física, caso a contratante não esteja dentro dos padrões mínimos recomendados nesse âmbito a contratada atua podendo indicar parceiros, instituições e/ou empresas que possam se responsabilizar com certos aspectos da proposta e realizar a implantação física e configuração de segurança, assim como o perímetro da sala de T.I. A isenção da implementação da segurança física se dá pelo modelo de negócio da ConsuTech, que possui foco em consultoria e soluções lógicas.

C) **Alocação dos recursos humanos e financeiros:** Para a implementação do Sistema de Gestão de Segurança da Informação (SGSI) na TechPro, estimamos um total de 500 horas de trabalho. Essa alocação inclui análise, planejamento, treinamento e execução das atividades relacionadas à segurança da informação; convertendo para uma perspectiva temporal:

- **Duração em Dias:** Considerando uma jornada de trabalho de 8 horas por dia, o projeto levará aproximadamente 62 dias.
- **Duração em Meses:** Se trabalharmos 20 dias por mês, o projeto será concluído em cerca de 3 meses.

Considerando o valor médio da hora de trabalho dos profissionais envolvidos, estabelecemos um custo de R$ 100,00 por hora. Esse valor leva em conta as habilidades específicas necessárias para a implementação do SGSI e a experiência dos colaboradores.

Os serviços oferecidos durante a implementação do SGSI incluem:

- **Análise de Riscos e Vulnerabilidades:** Identificação e avaliação das ameaças e vulnerabilidades específicas da TechPro; Priorização dos riscos com base na probabilidade e impacto.
- **Desenvolvimento de Políticas e Procedimentos:** Elaboração de políticas de segurança da informação alinhadas aos requisitos da ISO 27001; Definição de procedimentos para lidar com incidentes de segurança.
- **Treinamento e Conscientização:** Capacitação dos colaboradores sobre boas práticas de segurança; Sensibilização para a importância da proteção dos ativos de informação.
- **Implementação de Controles Técnicos:** Configuração de firewalls, antivírus e outras ferramentas de segurança; Monitoramento contínuo da rede e sistemas.
- **Auditoria e Certificação:** Realização de auditorias internas para verificar a conformidade com os padrões da ISO 27001; Preparação para a certificação oficial.

Lembrando que esses valores e serviços são estimativas iniciais e podem ser ajustados conforme a necessidade e complexidade do projeto.

Visando o atendimento aos requisitos da ISO 27001 mais cinco etapas se provam necessárias, que consistem em:

A) **Implementação dos controles de segurança:** visando atender as três etapas de gerenciamento (ações de prevenção, detecção e correção) e para melhor adequação da empresa as políticas de melhores práticas os controles de segurança foram divididos em três principais segmentos, sendo eles:

- **Controles administrativos:** Consistem em procedimentos e políticas que uma empresa implementa ao lidar com informações confidenciais. Nessa categoria as seguintes medidas serão implementadas:

  - Políticas e procedimentos de gerenciamento de ativos.
  - Políticas de renovação e força da senha.
  - Políticas e grupos de controle de acesso com base na função.
  - Políticas de renovação e força da senha.
  - Treinamento de usuários.
  - Crachás de funcionários.
  - Contratação de equipe de segurança especial.

- **Controles técnicos:** Envolvem hardwares e/ou softwares implementados para gerenciar riscos e oferecer proteção. Dentro deste contexto serão implementadas as seguintes medidas:
  - Controle de acesso a edifícios com base em cartão.
  - Proteção do sistema de dispositivos de rede.
  - VPN para trabalho remoto.
  - Criptografia de dados dos registros de clientes.
  - Backup de dados e do sistema operacional abrangente.
  - Firewalls de rede ou IPS.
  - Firewalls e antivírus baseados em host.
  - Contenção e remoção de malware.
  - Monitoramento de segurança de rede.

- Restauração de dados e imagens de disco do backup.
- Gerenciamento robusto de patches

- **Controles físicos:** São mecanismos como cercas e bloqueios implantados para proteger sistemas, instalações, pessoal e recursos. A ConsuTech elabora o projeto, porém, não se responsabiliza pela implementação de equipamentos para a conformidade dos controles físicos, podendo indicar quem a realize (vide **ANEXO A**). As seguintes medidas fazem parte dos controles físicos recomendados:

    - Acesso exclusivo do administrador ao data center e instalações de rede.
    - Avaliação de vulnerabilidade e teste de detecção.
    - Detectores de fumaça.
    - Sistemas de sprinklers.
    - Geradores de energia de backup para sistemas essenciais.
    - Monitoramento CFTV.
    - Manutenção regular de sistemas e equipamentos.
    - Substituição rápida de equipamentos essenciais danificados ou com mau funcionamento.
    - Inventário de peças sobressalentes.
    - Alarmes dos sensores de porta, janela e movimento.

B) **Desenvolvimento de procedimentos operacionais padrão (POP):** tem como objetivo proteger ativos de informação críticos e cumprir com as regulamentações aplicáveis além de ser um instrumento de apoio à padronização dos processos, visando minimizar erros, desvios e variações em processos. Este POP aplica-se a todos os departamentos e colaboradores da TechPro envolvidos na gestão de ativos de informação críticos, nele fica estabelecidas as instruções para criações de POPs subsequentes relacionados ao SGSI em cada setor da empresa. Para confecção de um procedimento operacional padrão a princípio deve-se realizar a avaliação e tratamento de riscos, o método a ser seguido é primeiro a identificação dos ativos críticos e em seguida a avaliação de ameaças e vulnerabilidades, realizados os dois procedimentos a equipe passa a listar as ameaças e vulnerabilidades da aplicação de tal procedimento e avaliar o potencial impacto de cada risco, a partir desta coleta faz-se a identificação e classificação de alternativas para

tratamentos dos riscos, com base nessas informações é desenvolvido um plano de implementação composto pelo plano detalhado e as responsabilidades de cada membro da equipe. As rotinas estabelecidas devem atender os requisitos da ISO 27001. A equipe de Implementação será composta pelo representante do comitê de segurança que será responsável pela supervisão e implementação do SGSI, o representante do departamento de TI que fara a identificação ativos de informação críticos e avaliação de ameaças e vulnerabilidades, o representante do setor de recursos humanos que por sua vez garantira a conformidade com a LGPD e outras regulamentações aplicáveis e os representantes de cada dos setores que serão encarregados de comunicar suas respectivas equipes sobre os procedimentos estabelecidos neste. Todas as políticas criadas devem ser revisadas periodicamente e caso necessário aprimoradas. Todo e qualquer novo POP relacionado ao SGSI deve seguir as etapas anteriormente descritas e ser aprovado pela equipe de implantação após apresentado para o comitê de segurança.

C) **Treinamento dos funcionários em segurança da informação:** para maior conscientização e conformidade com os procedimentos de segurança provou-se extremamente necessário o treinamento dos funcionários, de forma que o compartilhamento de conhecimento ocorra alinhado com as diretrizes da empresa para a adoção de estratégias futuras. Tendo isso em vista foram estabelecidos os seguintes treinamentos a serem realizados:

- **Treinamento interno:** Ocorre na empresa e é dividido em duas etapas, uma introdutória, fornecendo informações iniciais aos colaboradores quando eles entram na empresa, e outra de acompanhamento contínuo, para fortalecer e aplicar os conhecimentos ao longo do tempo.
- **Treinamento externo:** Será realizado fora do local de trabalho, através de palestras, workshops e cursos para complemento dos conhecimentos adquiridos nos treinamentos internos. Esse tipo de aprendizado proporcionara aos colaboradores o treinamento de especialistas específicos de suas áreas.

D) **Realização de avaliação de riscos regulares:** Empresas usam análise de riscos para avaliar os impactos causados por incidentes e assim poder garantir a eficiência do gerenciamento de riscos, garantir que as ações implementadas atendam todos os objetivos.
A ConsuTech segue uma premissa que o processo de análise deve ser orientado por alguns fatores que são pontos chaves para um troubleshooting eficaz.

- Identificação de ativos e seus valores.
- Identificação de ameaças e vulnerabilidades.
- Qualificação de ameaças identificadas o impacto que ela causa e a probabilidade de ocorrência.
- Impacto da ameaça X o custo operacional da contramedida.

Com esses pontos identificados seguimos para outros dois métodos que são pontos importantes no processo de avaliação de riscos a análise de risco quantitativa e a análise de risco qualitativa.

A análise quantitativa atribui números para o processo de análise tais como: Valor do ativo, custo de reposição do ativo, um ativo pode ter seu valor medido por receita adquirida pelo seu uso entre outros fatores. Nessa etapa do processo são levados em conta alguns pontos:

- **Fator de exposição:** É um valor subjetivo expresso como porcentagem, sendo contabilizado de 0,0 a 1,0 sendo 1,0 igual a 100%
- **Taxa anual de ocorrência:** É probabilidade de ocorrer uma perda durante o ano devido a um risco. Essa escala pode chegar a ser maior que 100% se um incidente ocorrer mais de 1 vez por ano.
- **Expectativa de perda anual:** Essa métrica dá uma perspectiva de quanto se deve investir para proteção de ativos.

Na análise qualitativa utiliza-se de cenários que possam descrever a probabilidade e o impacto de uma ameaça. Nela utilizamos uma matriz de riscos para quais riscos a organização precisa priorizar e quais respostas desenvolver. Os resultados da matriz são usados como guia para a empresa executar alguma ação mediante aos riscos.

E) **Avaliar os objetivos de controle e controles:** tem como objetivo identificar os resultados alcançados e compará-los com os resultados almejados, esse método ajuda a identificar desvios de projetos e assim ser possível reavaliar o projeto e implementar mudanças para alcançar as metas desejadas. O Uso de indicadores de metas são peças fundamentais para que se possamos chegar no resultado desejado através dos resultados dos indicadores é possível comparar o resultado real com os objetivos, analisar os desvios e tomar uma ação corretiva com os resultados obtidos. Esse processo é importante pois através dele será possível fazer um acompanhamento das ações tomadas e avaliar a eficiência das ações e gerar aprendizado organizacional para revisões no próprio planejamento. Com isso o objetivo desta avaliação é garantir que o projeto inicial alcance as metas estabelecidas de forma que identifique falhas, para que ações sejam tomadas para corrigi-las e com isso gerar aprendizado para a organização e o projeto em revisões futuras.

Com base no anexo A da ISO 27001 foram estabelecidos os objetivos de controle e controles deste SGSI, sendo eles:

- A.5 Políticas de segurança da informação – controles sobre como as políticas são escritas e revisadas.
- A.6 Organização da segurança da informação – controles sobre como as responsabilidades são designadas; também inclui os controles para dispositivos móveis e trabalho remoto.
- A.7 Segurança em recursos humanos – controles para antes da contratação, durante e após a contratação.
- A.8 Gestão de ativos – controles relacionados ao inventário de ativos e uso aceitável, e para a classificação de informação e manuseio de mídias.
- A.9 Controle de acesso – controles para a política de controle de acesso, gestão de acesso de usuários, controle de acesso a sistemas e aplicações, e responsabilidades dos usuários.
- A.10 Criptografia – controles relacionados a gestão de chaves criptográficas.
- A.12 Segurança nas operações – vários controles relacionados a gestão da produção de TI: gestão de mudança, gestão de capacidade, software malicioso, cópia de segurança, registro de eventos, monitoramento, instalação, vulnerabilidades, etc.
- A.13 Segurança nas comunicações – controles relacionados a segurança em rede, segregação, serviços de rede, transferência de informação, mensageiria, etc.

- A.14 Aquisição, desenvolvimento e manutenção de sistemas – controles definindo requisitos de segurança e segurança em processos de desenvolvimento e suporte.
- A.12 Segurança nas operações – vários controles relacionados a gestão da produção de TI: gestão de mudança, gestão de capacidade, software malicioso, cópia de segurança, registro de eventos, monitoramento, instalação, vulnerabilidades, etc.
- A.13 Segurança nas comunicações – controles relacionados a segurança em rede, segregação, serviços de rede, transferência de informação, mensageiria, etc.
- A.14 Aquisição, desenvolvimento e manutenção de sistemas – controles definindo requisitos de segurança e segurança em processos de desenvolvimento e suporte.

ANEXO A (ESTRUTURA DE REDE FÍSICA INDICADA)

ITEM 0 – RACK PARA MONTAGEM SERVIDOR: Dell APC Rack NetShelter SX 42U 19" 600mm x 1070mm;

ITEM 1 - CABEAMENTO CAT6: 1 caixa com 300 metros, Furukawa;

ITEM 2 – LINK 1 PRINCIPAL: Internet dedicada com redundância de 1 GBps;

ITEM 3 – LINK 2 BACKUP: Redundância de Internet Banda Larga de até 1 GBPs;

ITEM 4 – FIREWALL FORTINET: Proteção DDoS, IDS/IPS, balanceamento de carga de rede, regras de entrada e saída, restrições de acesso por localidade;

ITEM 5 – SWITCH GERENCIÁVEL 48PT. GIGABIT: Criação de VLAN por setor para otimização do tráfego de rede, gerenciamento e liberação de portas;

ITEM 6 – SERVIDOR DE ARQUIVOS: Computador com armazenamento de até 10TB, com RAID ativo – espelhamento de HD, redundância de fonte de energia – troca quente, criptografia dos dados e rotinas de backup automatizadas.

ITEM 7 – SERVIDOR DE APLICAÇÃO + AUTENTICAÇÃO: Máquina específica para comportar o sistema de SGSI

ITEM 8 – 2 NOBREAKS DE 5000VA + MÓDULO EXTERNO COM 2 BATERIAS DF500: Equipamento para suportar queda de energia da estrutura por até 5 horas

ITEM 9 – DVR SISTEMA DE CÂMERAS PARA VISIBILIDADE DA ESTRUTURA FÍSICA DA REDE: Cameras externas posicionadas na entrada da sala + cameras internas da sala de T.I.

ITEM 10 – CONTROLE DE ACESSO FACIAL OU POR CARTÃO PARA ENTRADA RESTRITA