ISEP INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO

Assignment 3. Security plan

João Figueiredo, 1230194
João Araújo, 1200584
Diogo Magalhães, 1201100

Curso: Mestrado em Engenharia Informática
Disciplina: Segurança de Sistemas de Informação (SEGSI)

Professor: Jorge Pinto Leite

Data: Dezenbro, 2023

Ano académico: 2023/2024

Conteúdo

Lista de Figuras

Capítulo 1

Introdução

1.1 Contexto

Em resposta à política de ciberdefesa da União Europeia (UE), este plano de segurança é uma obrigação para organizações, procurando alinhar-se às diretrizes estabelecidas pela mesma. No panorama atual, em que a ligação digital é a norma, a necessidade de salvaguardar recursos digitais torna-se crucial. Este contexto desafia as organizações a desenvolverem estratégias abrangentes que não apenas cumpram, mas ultrapassem as expectativas delineadas pela política de ciberdefesa da UE.

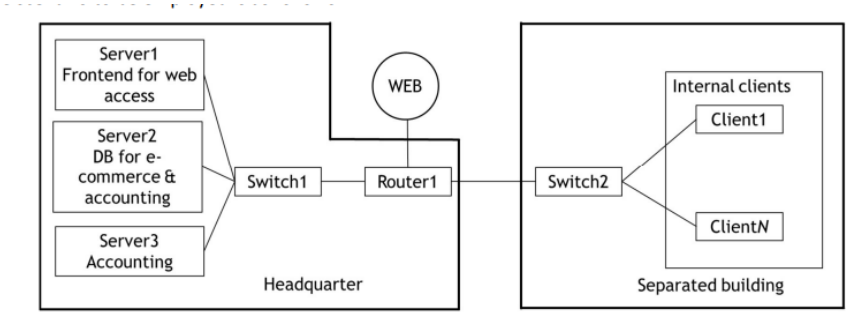

Figura 1.1: Cenário da empresa

1.2 Objetivos

1.2.1 Definição e Proposição do Plano de Segurança

O objetivo primordial deste plano é definir e propor uma estrutura de segurança que atenda aos requisitos e padrões estabelecidos pela política de ciberdefesa da UE. Isso envolve a criação de componentes-chave, desde a Política Geral de Segurança até a gestão de ativos, gestão de riscos, gestão de incidentes e a implementação de controlos técnicos e físicos, conforme apropriado.

1.2.2 Alinhamento com as Diretrizes da UE

Garantir que todas as medidas propostas estejam alinhadas de maneira consistente com as diretrizes e regulamentações da UE. Isso inclui não apenas atender aos requisitos mínimos, mas também buscar a excelência na implementação de práticas recomendadas e estratégias de segurança proativas.

1.2.3 Coerência entre as Componentes do Plano

Manter uma abordagem coesa e integrada ao desenvolver cada componente do plano é fundamental para garantir a eficácia global das estratégias de segurança.

1.3 Estrutura do Documento

No documento a ser desenvolvido, todos as componentes do plano de segurança irão ser descritas.

1.3.1 Política Geral de Segurança

Aqui, apresentamos a base do nosso plano, a Política Geral de Segurança, que define a intenção e o propósito da organização relativamente à segurança da informação.

1.3.2 Inventário de Ativos

Detalhamos como identificamos, categorizamos e gerimos ativos (digitais e físicos) para garantir a sua integridade, confidencialidade e disponibilidade.

1.3.3 Gestão de Riscos

Descrevemos o processo de identificação, avaliação e mitigação de riscos, assegurando que estejamos proativamente protegendo os nossos ativos contra ameaças potenciais.

1.3.4 Gestão de Incidentes

Esta secção delimita os procedimentos para responder efetivamente a incidentes de segurança, minimizando danos e restaurando a normalidade operacional.

1.3.5 Medidas Técnicos e Físicos

Quando aplicável, apresentamos as medidas técnicas e físicas implementadas para fortalecer as nossas defesas contra ameaças cibernéticas.

1.4 Organização do Trabalho

O projeto está estruturado em 5 capítulos, abordando os seguintes temas: Plano Geral de Segurança, Inventário de Ativos, Gestão de Risco, Gestão de Incidentes, e Controles Técnicos e Físicos.

Cada membro do grupo foi responsável por uma parte específica do trabalho, distribuindo as tarefas conforme as suas habilidades e competências. A colaboração efetiva de cada integrante foi fundamental para a elaboração abrangente e coerente deste projeto de segurança.

A seguir, um resumo das responsabilidades de cada membro:

1. **Capítulo 2 - Plano Geral de Segurança:** [João Figueiredo]
2. **Capítulo 3 - Inventário de Ativos:** [João Figueiredo]
3. **Capítulo 4 - Gestão de Risco:** [João Araújo]
4. **Capítulo 5 - Gestão de Incidentes:** [Diogo Magalhães]
5. **Capítulo 6 - Controles Técnicos e Físicos:** [Diogo Magalhães / João Araújo]

A contribuição individual de cada integrante enriqueceu o projeto, resultando num plano de segurança abrangente e bem elaborado.

Capítulo 2

Política Geral de Segurança

2.1 Introdução

A Empresa XPTO reconhece a importância crucial da implementação de medidas de segurança para aprimorar a sua operação, competitividade e responsabilidade social. Conforme a legislação vigente e a necessidade de assegurar a Segurança da Informação (SI) e da Infraestrutura, a Empresa XPTO apresenta a sua política de segurança baseada nos requisitos da norma internacional ISO 27001.

2.2 Objetivos

A política de segurança da Empresa XPTO tem como principal objetivo proporcionar um ambiente seguro e confiável para todos os stakeholders, assegurando a continuidade dos negócios e o cumprimento das obrigações legais. Para atingir esses objetivos, a Empresa XPTO compromete-se a:

a) Garantir um nível adequado de segurança da rede e informação, oferecendo transparência, confiança e serviços eficientes a parceiros e colaboradores.

b) Aumentar a eficácia e eficiência dos processos internos da Segurança da Informação (SI).

c) Identificar, avaliar e controlar, de forma contínua, os riscos e vulnerabilidades dos ativos de tratamento da informação.

d) Estabelecer políticas e procedimentos que garantam disponibilidade, integridade e confidencialidade das informações, conforme requisitos de negócio, leis e regulamentos.

e) Garantir a adequação e exequibilidade da política de segurança, com melhorias contínuas planeadas ou em resposta a alterações relevantes na Organização.

f) Assegurar recursos para operacionalização dos processos e atividades na gestão da Segurança, incluindo a sensibilização/formação dos colaboradores, parceiros e clientes nesta área.

2.3 Implementação

Além disso, a implementação dos objetivos incluirá:

- **Avaliações de Risco Contínuas:** Realizar avaliações de risco regulares para identificar novas ameaças e vulnerabilidades.
- **Melhoria Contínua:** Estabelecer um ciclo de melhoria contínua, revendo regularmente as práticas de segurança e implementando melhorias conforme necessário.

As políticas e procedimentos estão presentes em todos os níveis da organização, com foco nos seguintes objetivos:

- Assegurar conformidade com a última versão da norma ISO/IEC 27001 durante a revisão da presente política.

- Garantir confidencialidade, integridade e disponibilidade de informações, serviços e infraestruturas em situações normais e excecionais.
- Garantir compreensão e cumprimento efetivo das medidas de segurança por todos os empregados.
- Cumprir requisitos legais e regulamentares aplicáveis nos processos e políticas de Segurança da Informação.
- Minimizar o número de incidentes de segurança e garantir resolução dentro do prazo estabelecido.

2.4 Segurança Contínua

A promoção de uma cultura de segurança contínua é essencial para fortalecer as defesas da organização contra ameaças em constante evolução. A segurança contínua vai além de simplesmente implementar medidas iniciais; ela representa um compromisso constante com a adaptação, aprendizagem e desenvolvimento contínuo. Neste contexto, abordamos diversos aspetos cruciais para garantir uma segurança eficaz a longo prazo:

2.4.1 Adoção de Soluções Técnicas Avançadas.

A rápida evolução das ameaças digitais exige que a organização adote soluções técnicas avançadas. Isso inclui a implementação de firewalls modernos, sistemas de deteção e prevenção de intrusões, antivírus atualizados e outras ferramentas de segurança de última geração. Manter-se atualizado com as mais recentes tecnologias é fundamental para garantir a eficácia das defesas contra ameaças digitais em constante desenvolvimento.

2.4.2 Medidas Organizacionais Proativas

Além das soluções técnicas, é crucial implementar medidas organizacionais proativas. Isso envolve a criação de políticas de segurança claras, a designação de responsabilidades específicas para a gestão da segurança, e a realização de auditorias regulares para garantir a conformidade com as políticas estabelecidas. A colaboração entre as diferentes equipas na organização é essencial para garantir uma abordagem holística à segurança.

2.4.3 Formações e Sensibilizações Constantes

A formação contínua é uma pedra angular da segurança contínua. Todos os membros da organização, desde funcionários até gestores, devem receber treino regular sobre práticas de segurança, reconhecimento de ameaças e procedimentos de resposta a incidentes. A sensibilização contínua para questões de segurança ajuda a criar uma mentalidade vigilante em todos os níveis da organização, tornando-a mais resistente a ataques.

2.4.4 Alinhamento com Padrões Internacionais (ISO 27001)

O alinhamento com padrões internacionais, como ISO 27001, fornece uma estrutura sólida para a implementação e gestão eficaz da segurança da informação. A conformidade com esses padrões não apenas fortalece as práticas de segurança, mas também estabelece a confiança com partes interessadas externas, como clientes e parceiros de negócios.

2.4.5 Melhoria Contínua dos Processos de Negócio

A segurança contínua não se limita apenas ao ambiente tecnológico; ela abrange todos os processos de negócio. A organização deve estar constantemente revendo e melhorando os seus procedimentos operacionais para garantir que a segurança seja incorporada em todas as atividades. Isso pode incluir revisões regulares de políticas, procedimentos de resposta a incidentes e planos de continuidade de negócios.

2.4.6 Aperfeiçoamento das Equipas de Segurança da Informação

Investir no desenvolvimento contínuo das equipas de Segurança da Informação é crucial. Isso envolve proporcionar oportunidades de formação especializada, participação em conferências e workshops relevantes, e a criação de um ambiente que incentive a partilha de conhecimentos e a colaboração. Equipas bem treinadas e informadas são essenciais para manter a segurança em constante evolução.

A segurança contínua não é apenas uma medida de proteção; é um componente vital para o sucesso sustentável da organização num ambiente digital em constante transformação. Ao adotar uma mentalidade de segurança contínua, a organização se posiciona de forma mais resiliente contra ameaças emergentes e desafios de segurança. Isso não é apenas um investimento na segurança da informação, mas também na sustentabilidade e no crescimento a longo prazo da organização.

2.5 Políticas Sectoriais

As Políticas Setoriais são componentes essenciais da Política Geral de Segurança da Empresa XPTO, abordando áreas específicas da organização. Desenvolvidas conforme padrões e regulamentos, essas políticas fornecem direcionamento claro para práticas operacionais, contribuindo para uma base sólida de segurança. Atuando em conjunto, formam uma rede coesa de diretrizes que abrangem diversas facetas da operação, promovendo um ambiente seguro. A implementação bem-sucedida protege ativos críticos, dados sensíveis e assegura a conformidade com normas regulamentares, fortalecendo a postura global de segurança e mitigando riscos em toda a organização.

2.6 Data de Implementação e Dúvidas

Esta política entra em vigor em 7 de janeiro de 2024. Em caso de dúvidas sobre a implementação deste plano de segurança, solicita-se que as mesmas sejam encaminhadas ao Chief Information Security Officer (CISO) da empresa.

Para esclarecimentos ou questionamentos relacionados a esta política, entre em contato com Carlos Alberto, CISO, através do seguinte canal:

Nome: Carlos Alberto
Cargo: Chief Information Security Officer (CISO)
E-mail: CarlosAlberto@isep.ipp.pt
Telefone: 961234567

A colaboração de todos os funcionários é fundamental para garantir o cumprimento efetivo desta política e a segurança da informação em nossa empresa.

Capítulo 3

Inventário de Ativos

3.1 Introdução

O Inventário de Ativos é uma parte integral da estratégia de segurança da Empresa XPTO, fornecendo uma visão abrangente e organizada de todos os recursos relevantes para as operações. Este capítulo destina-se a definir os procedimentos e informações associadas ao Inventário de Ativos, destacando a sua importância na gestão eficaz da segurança da informação.

3.2 Definição de Ativos

Para os fins deste inventário, consideramos ativos como qualquer recurso fundamental para as operações, incluindo hardware, software, dados e equipamentos.

3.3 Escopo do Inventário

O inventário abrange todos os ativos da Empresa XPTO, incluindo aqueles localizados em instalações físicas, na rede interna e aqueles acessíveis pela Internet. O escopo detalhado está definido conforme as diretrizes das autoridades nacionais.

3.4 Responsabilidades

A responsabilidade pelo Inventário de Ativos é atribuída às equipas dos diversos departamentos da empresa XPTO. Cada ativo tem um responsável designado, conforme indicado na coluna "Responsável"da lista.

3.5 Processo de Inventário

O processo de inventário consiste em identificação, documentação e atualização contínua dos ativos. A revisão do inventário ocorre [especifique a frequência] para garantir a precisão das informações.

3.6 Classificação de Ativos

Os ativos são classificados com base em critérios como confidencialidade, integridade e disponibilidade. Essas classificações são fundamentais para determinar os níveis de segurança associados a cada ativo.

3.7 Informações Contidas no Inventário

Cada ativo é registado com informações como número de inventário, modelo, número de série/licença, localização física, endereço IP e MAC (quando aplicável).

3.8 Proteção do Inventário

A proteção do Inventário de Ativos é uma prioridade fundamental para garantir a confiabilidade e segurança das informações contidas. Diversas medidas de segurança são implementadas visando resguardar a integridade, confidencialidade e disponibilidade dos dados armazenados no inventário. Estas medidas são cuidadosamente projetadas para mitigar potenciais ameaças e assegurar que somente pessoal autorizado tenha acesso às informações sensíveis.

3.8.1 Controle de Acesso

Um robusto sistema de controle de acesso é implementado para regular a entrada ao Inventário de Ativos. Isso inclui a atribuição de credenciais exclusivas a utilizadores autorizados, com níveis de permissão devidamente definidos de acordo com suas responsabilidades. Além disso, é estabelecido um protocolo de autenticação forte para garantir a identificação segura dos utilizadores.

3.8.2 Criptografia de Dados

Todas as informações sensíveis armazenadas no Inventário de Ativos são submetidas a processos de criptografia avançada. Isso assegura que, mesmo em caso de acesso não autorizado, os dados permaneçam ininteligíveis, protegendo a confidencialidade das informações críticas.

3.8.3 Backup e Recuperação

Procedimentos eficazes de backup são estabelecidos para garantir a preservação dos dados no caso de eventos inesperados, como falhas de sistema, ataques cibernéticos ou desastres naturais. Além disso, são implementados planos de recuperação para restaurar rapidamente o acesso e funcionalidade em situações adversas.

3.8.4 Formação em Segurança

O pessoal envolvido na administração e acesso ao Inventário de Ativos passa por formações regulares em segurança da informação. Esses programas visam informar sobre práticas seguras, procedimentos de acesso e a importância de manter a integridade do inventário.

3.9 Auditoria

Auditorias periódicas do inventário serão conduzidas para verificar a sua precisão.

3.10 Documentação de Políticas Relacionadas

Este inventário é alinhado com as políticas gerais de segurança da Empresa XPTO, garantindo coesão e consistência em toda a estratégia de segurança.

3.11 Inventário de ativos da Empresa XPTO

A seguir, apresentamos a lista de inventários de ativos da Empresa XPTO, elaborada para análise e documentação. O documento detalhado, ficheiro excel, com os ativos está anexado a este relatório para referência.

Capítulo 4

Gestão de risco

A gestão de riscos é um processo sistemático que envolve identificar, avaliar, priorizar e mitigar riscos para atingir os objetivos das organizações. É um aspeto importante da estratégia de uma empresa no contexto da segurança da informação e da cibersegurança.
Existem 8 fases da gestão de riscos (Fig.4.1), normalmente fazem parte de um processo abrangente que pretende identificar, avaliar e mitigar riscos para garantir a segurança de uma organização ou sistema. Estas fases ajudam as empresas a abordar sistematicamente potenciais ameaças e vulnerabilidades.

4.1 Processo de identificação de riscos

1. **Estabelecer o contexto:** Neste passo, é fundamental compreender o ambiente em que o plano de segurança será implementado. Isso envolve identificar as metas e objetivos do plano, as partes interessadas, as regulamentações aplicáveis, e outros fatores que possam influenciar a gestão de riscos.

2. **Identificação de risco:**

   - É a primeira fase real da fase de avaliação do risco
     - **Identificação ativa:** Aqueles que suportam o escopo definido na gestão de riscos de segurança da informação
     - **Identificação de vulnerabilidades:** Identificação e seleção das vulnerabilidades relacionadas a cada dispositivo
     - **Identificação de ameaças:** Para cada vulnerabilidade, identificar e selecionar as potenciais ameaças
     - **Controla a identificação:** Identificar controlos existentes, descrevendo a sua maturidade de implementação e/ou uso
     - **Avaliar o impacto geral:** Pode incluir consequências potenciais, como tempo necessário para investigar e reparar, tempo de trabalho desperdiçado, etc.

3. **Análise de risco:** Na análise de risco, a equipa avalia a probabilidade de ocorrência e o impacto potencial de cada risco identificado. A análise deve ser qualitativa, ou quantitativa, atribuindo valores numéricos. Essa etapa permite uma compreensão mais profunda dos riscos e ajuda na priorização.

4. **Avaliação de risco:** Com base na análise de risco, os riscos são classificados em termos de sua criticidade. Isso possibilita que a empresa priorize os riscos e agrupe os seus recursos naqueles que representam as maiores ameaças ou têm o potencial de causar os maiores danos.

5. **Tratamento do risco:** No tratamento do risco, a empresa desenvolve estratégias para lidar com cada risco identificado nos passos anteriores. Isto deve incluir aceitar o risco, mitiga-lo reduzindo a probabilidade ou o impacto, transferir o risco através de seguros ou parcerias, ou evitar completamente o risco através de alterações nas práticas ou tecnologias.

6. **Comunicação e consulta do risco:** A comunicação eficaz é essencial para assegurar que todas as partes interessadas estejam informadas dos riscos e das estratégias de tratamento. Envolve partilhar informações sobre os riscos identificados e as medidas de segurança implementadas de forma a garantir que todos estejam em atualizados.

7. **Revisão e acompanhamento do risco:** A gestão de riscos é um processo dinâmico que requer revisão contínua. A organização deverá acompanhar regularmente os riscos identificados, avaliar a eficácia das estratégias de tratamento e ajustar suas abordagens conforme necessário. Mudanças no ambiente da empresa podem exigir atualizações no plano de segurança.

8. **Documentação do processo:** A documentação detalhada de todo o processo da gestão de riscos é fundamental para as empresas. Esta deve incluir os registos dos riscos identificados ao longo de todo o processo de gestão de riscos, as análises efetuadas, estratégias de tratamento decididas, resultados das avaliações e revisões. A documentação serve como uma forma de histórico e como nota para possíveis análises de riscos a ter em conta mais tarde.

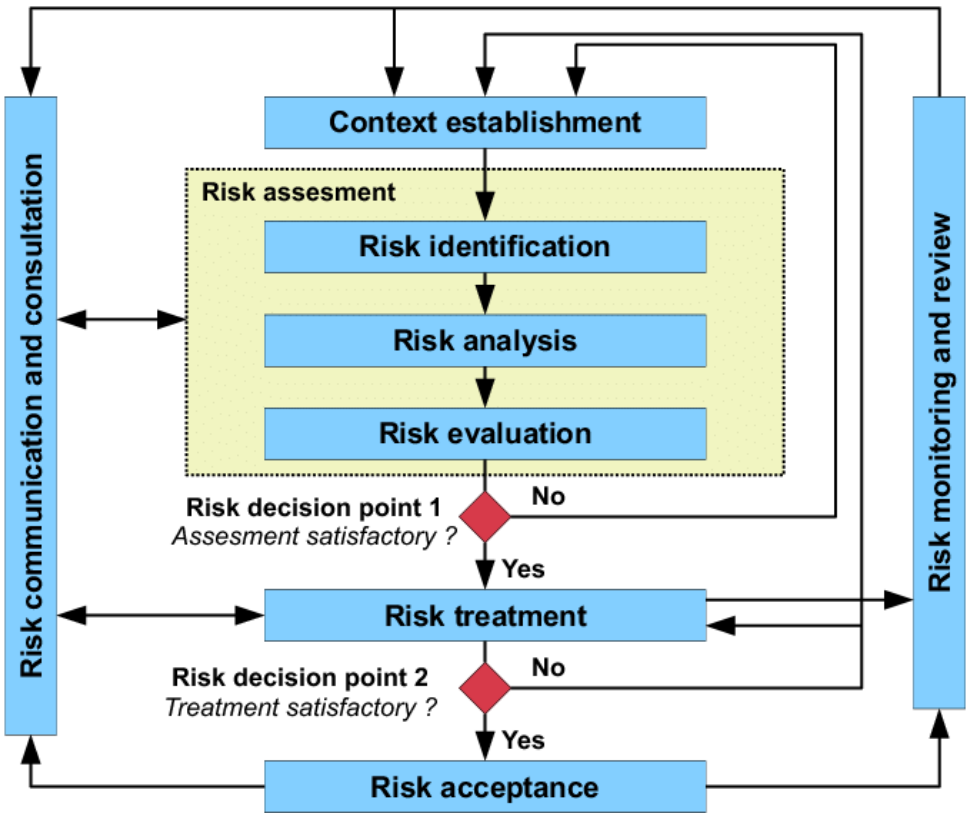

Figura 4.1: Gestão de risco

4.2 Riscos:

- **Risco de Ataques Cibernéticos Sofisticados:**
  - **Descrição:** Com a crescente sofisticação dos ataques cibernéticos, as organizações podem enfrentar ameaças avançadas, como ataques de 'ransomware', 'malware' de última geração e ações de 'phishing' cada vez mais persuasivos. Esses ataques podem ser direcionados a sistemas críticos, dados sensíveis e infraestruturas essenciais.
  - **Impacto Potencial:** Perda de dados confidenciais, interrupção de serviços, danos à reputação da empresa, e potencial exposição a sanções legais.

- **Risco de Ataques de Rede Interna:**

- **Descrição:** A presença de servidores, 'switches' e 'routers' cria uma rede interna que pode ser alvo de ataques de 'insiders´ ou aparelhos comprometidos dentro da organização. A falta de controlos adequados pode permitir acesso não autorizado aos servidores ou manipulação de tráfego interno, comprometendo a integridade e confidencialidade dos dados.
- **Impacto Potencial:** Exposição de dados sensíveis, interrupção de serviços críticos, possíveis violações de conformidade e danos à reputação da empresa.

- **Risco de Falha na Conectividade entre Edifícios:**
  - **Descrição:** A comunicação crítica entre os edifícios, realizada por meio do 'router' e 'switches' associados, apresenta o risco de falha na conectividade. Problemas como interrupções na linha de comunicação, falhas no equipamento de rede, etc. podem resultar em perda de comunicação entre os edifícios.
  - **Impacto Potencial:** Interrupção da colaboração entre os edifícios, atraso na transferência de dados, comprometimento da continuidade operacional e dificuldades no acesso a recursos partilhados.

Capítulo 5

Gestão de incidentes

5.1 Introdução

A gestão de incidentes desempenha um papel crítico na segurança da informação, garantindo que a empresa XPTO esteja preparada para responder efetivamente a eventos de segurança. Este capítulo aborda os procedimentos e estratégias para lidar com incidentes de segurança, minimizando danos e restaurando a normalidade operacional. Para os propósitos deste plano, um incidente de segurança é definido como qualquer evento que comprometa a confidencialidade, integridade ou disponibilidade dos ativos de informação da empresa XPTO

5.2 Processo de Resposta a Incidentes

1. **Deteção:** A deteção de incidentes é fundamental. Todos os funcionários têm a responsabilidade de relatar qualquer atividade suspeita. A organização implementará ferramentas de monitorização avançadas para identificar anomalias e alertar sobre possíveis incidentes.

2. **Avaliação:** Uma vez detetado, o incidente é avaliado quanto à sua gravidade, potencial impacto e origem. Essa avaliação é realizada por uma equipa designada de resposta a incidentes, que determinará a melhor abordagem para mitigação.

3. **Mitigação:** Ações imediatas são tomadas para conter e minimizar o impacto do incidente. Isso pode incluir isolar sistemas afetados, desativar contas comprometidas ou aplicar medidas de segurança adicionais.

4. **Investigação:** Uma investigação detalhada é conduzida para entender a origem do incidente, identificar vulnerabilidades exploradas e coletar evidências para futuras ações legais, se necessário.

5. **Comunicação:** A comunicação efetiva é essencial durante um incidente. A equipa de resposta manterá todas as partes interessadas informadas sobre o progresso, impacto e medidas tomadas. Isso incluirá comunicação interna e externa, conforme apropriado.

6. **Recuperação:** Após a contenção do incidente e conclusão da investigação, o processo de recuperação é iniciado. Isso envolve a restauração de sistemas afetados, a implementação de melhorias de segurança e a revisão de políticas e procedimentos.

5.3 Processo de Resposta a Incidentes

5.3.1 Risco de Ataques Cibernéticos Sofisticados

- **Deteção:**
  - Utilizar ferramentas avançadas de deteção de ameaças e sistemas de monitorização para identificar padrões ou atividades incomuns que possam indicar um ataque cibernético sofisticado.
  - Implementar sistemas de deteção de intrusão e anomalias para identificar possíveis ameaças cibernéticas de forma proativa.
- **Avaliação:**
  - Avaliar a gravidade da ameaça detetada com base no impacto potencial e na probabilidade de exploração bem-sucedida.
  - Priorizar a resposta com base na gravidade dos sistemas afetados, concentrando-se nos elementos mais críticos.
- **Mitigação:**
  - Isolar imediatamente sistemas ou redes afetados para evitar a propagação da ameaça cibernética dentro da infraestrutura.
  - Implementar medidas temporárias para mitigar o impacto enquanto a investigação detalhada do ataque está em andamento.
- **Investigação:**
  - Conduzir uma análise minuciosa do ataque cibernético, investigando a origem, métodos utilizados e as vulnerabilidades potenciais exploradas.
  - Identificar a extensão da violação e dos sistemas afetados para compreender totalmente o impacto do ataque.
- **Comunicação:**
  - Notificar imediatamente as partes interessadas relevantes sobre o incidente, fornecendo informações claras acerca da natureza do ataque e das medidas tomadas para mitigar os seus impactos.
  - Manter linhas de comunicação abertas para fornecer atualizações regulares sobre os esforços de resposta ao incidente.
- **Recuperação:**
  - Restaurar sistemas e serviços afetados após garantir que a ameaça tenha sido totalmente erradicada e os sistemas estejam seguros.
  - Implementar medidas de segurança adicionais para fortalecer a postura de segurança e prevenir possíveis ocorrências futuras de ataques cibernéticos sofisticados.

5.3.2 Risco de Ataques de Rede Interna

- **Deteção:**
  - Monitorizar continuamente as atividades na rede interna, visando detetar qualquer sinal de acesso não autorizado ou comportamento incomum.
  - Implementar análise de comportamento de utilizadores para identificar anomalias nas atividades, destacando potenciais ameaças internas ou dispositivos comprometidos.
- **Avaliação:**
  - Avaliar o impacto da violação na integridade, confidencialidade dos dados e conformidade com regulamentações pertinentes.
  - Priorizar a resposta com base na gravidade dos serviços afetados, dando atenção especial aos elementos críticos.
- **Mitigação:**
  - Isolar imediatamente dispositivos ou secções comprometidas na rede interna para conter a propagação da ameaça.
  - Implementar controlos temporários para minimizar danos adicionais enquanto se investiga e resolve o incidente.
- **Investigação:**
  - Conduzir uma investigação detalhada para determinar a origem da violação da rede interna, identificando se foi uma ameaça interna ou um dispositivo comprometido.
  - Identificar e corrigir as vulnerabilidades que permitiram a violação, fortalecendo a segurança da rede contra futuros ataques.
- **Comunicação:**
  - Comunicar de imediato o incidente às partes interessadas relevantes, incluindo equipas internas e de gestão, garantindo transparência e colaboração.
  - Fornecer orientações claras sobre medidas de segurança adicionais para prevenir incidentes semelhantes no futuro.
- **Recuperação:**
  - Restaurar completamente os componentes e serviços afetados na rede interna, assegurando a retoma da operacionalidade normal.
  - Reforçar as medidas de segurança na rede interna, implementando melhorias com base nas lições aprendidas durante o incidente para evitar recorrências.

5.3.3 Risco de Falha na Conectividade entre Edifícios

- **Deteção:**
  - Implementar sistemas de monitorização avançados para detetar qualquer interrupção ou comportamento anómalo na conectividade da rede entre edifícios. Isso pode incluir soluções automatizadas que alertam imediatamente em caso de falha ou degradação da rede.
  - Utilizar ferramentas de avaliação da saúde da rede para identificar possíveis problemas antes que afetem significativamente a conectividade.
- **Avaliação:**
  - Realizar uma avaliação abrangente do impacto da falha na conectividade, considerando a colaboração entre edifícios, a transferência de dados críticos e a continuidade operacional.
  - Priorizar a resposta com base na gravidade dos canais de comunicação afetados, dando ênfase à rápida resolução dos elementos mais críticos.
- **Mitigação:**
  - Isolar imediatamente os canais de comunicação afetados para evitar uma propagação maior das interrupções.
  - Implementar medidas temporárias para garantir um impacto mínimo durante o período de investigação, o que pode incluir a configuração de rotas alternativas de comunicação.
- **Investigação:**
  - Conduzir uma investigação aprofundada para identificar a causa raiz da falha na conectividade. Isso envolve examinar possíveis problemas de hardware, investigar potenciais ataques à rede e avaliar questões de infraestrutura que possam ter contribuído para a interrupção.
  - Determinar a extensão da perda de comunicação entre edifícios, avaliando o alcance total do incidente.
- **Comunicação:**
  - Comunicar prontamente o incidente aos ocupantes dos edifícios afetados, garantindo transparência e oferecendo orientações claras sobre como proceder.
  - Fornecer atualizações regulares sobre o status do incidente e o progresso dos esforços de resolução, mantendo todas as partes interessadas informadas.
- **Recuperação:**
  - Restaurar integralmente os canais de comunicação entre edifícios, implementando medidas corretivas com base nas conclusões da investigação.
  - Reforçar a resiliência da infraestrutura de interconexão através da implementação de medidas adicionais de segurança e redundância.

Capítulo 6

Controlos Técnicos e Físicos

6.1 Contexto:

No cenário dinâmico da cibersegurança moderna, a empresa XPTO emprega uma abordagem multifacetada para proteger os seus ativos e informações confidenciais. Uma medida fundamental num plano de segurança é o controlo técnico e físico.

- **Controlos Técnicos:** Os controlos técnicos abrangem um conjunto diversificado de salvaguardas tecnológicas concebidas para gerir e restringir o acesso a sistemas e dados digitais. Esses controlos aproveitam software e tecnologias de rede para defesa contra acesso não autorizado, violações de dados, etc. Mecanismos de autenticação, firewall's e sistemas de deteção de intrusões estão entre os principais componentes que constituem a base dos controlos técnicos.
- **Controlos Físicos:** Os controlos físicos, por outro lado, concentram-se na salvaguarda dos ativos tangíveis e da infraestrutura da empresa XPTO. Esses controlos visam impedir o acesso físico não autorizado a edifícios, etc. Medidas como sistemas de controlo de acesso e câmaras de vídeo-vigilância constituem um papel importante na segurança física.

6.2 Técnicas de Controlo

6.2.1 Ataques Cibernéticos Sofisticados

- **Controlos Técnicos:**
  - **Firewall's Avançadas:** Utilização de firewall's avançadas para filtrar tráfego indesejado e identificar padrões de ataque.
  - **Soluções de Deteção e Prevenção de Intrusões:** Implementação de sistemas de soluções de deteção e prevenção de intrusões para acompanhar e responder a atividades suspeitas na rede.
  - **Soluções de Antivírus e Anti-malware:** Utilização de software de segurança para proteger contra malware e ameaças conhecidas.
  - **Gestão de Acesso:** Implementação de políticas de controlo de acesso para garantir que apenas utilizadores autorizados tenham acesso a sistemas críticos.
  - **Criptografia:** Uso de criptografia para proteger dados sensíveis durante a transmissão e armazenamento.
- **Controlos Físicos:**
  - **Backup e Armazenamento Seguro:** Manutenção de cópias de backup em locais físicos seguros para recuperação de dados em caso de comprometimento.

6.2.2 Ataques de Rede Interna

- **Controlos Técnicos:**
  - **Encriptação:** A encriptação transforma os dados em um formato seguro que só pode ser lido por quem tiver a chave de desencriptação apropriada. Ajuda a proteger informações sensíveis durante a transmissão e o armazenamento.
  - **Multi-Factor Authentication (MFA):** A MFA requer que os utilizadores forneçam dois ou mais fatores de verificação (por exemplo, palavra-passe e código de uso único) para obterem acesso, adicionando uma camada extra de segurança.
- **Controlos Físicos:**
  - **Câmaras de vigilância:** As câmaras de vigilância são utilizadas para acompanhar e registar atividades em espaços físicos. Reforçam a segurança, fornecendo um registo visual dos acontecimentos.
  - **Sistemas de cartões de acesso:** Os cartões de acesso utilizam chips incorporados ou bandas magnéticas para conceder ou restringir a entrada em áreas seguras. O acesso pode ser controlado através da configuração das permissões do leitor de cartões.

6.2.3 Falha na Conectividade entre Edifícios

- **Controlos Técnicos**
  - **Caminhos de rede redundantes:** O estabelecimento de caminhos de rede redundantes garante que, se um caminho falhar, o tráfego pode ser redirecionado automaticamente através de um caminho alternativo, minimizando o tempo de inatividade.
  - **Dispositivos de rede de alta disponibilidade:** Usar dispositivos de rede com recursos de alta disponibilidade, como fontes de alimentação e componentes redundantes, para minimizar o risco de falhas no dispositivo.
- **Controlos Físicos**
  - **Medidas de segurança física:** Proteção física da infraestrutura de rede através da implementação de medidas de segurança, tais como acesso restrito a salas e equipamentos de rede.
  - **Roteamento de caminhos diversos:** Diversificar fisicamente os caminhos da rede, como usar diferentes caminhos para os cabos de rede, reduz o risco de um único ponto de falha.