P.PORTO

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Licenciatura em Segurança Informática em Redes de Computadores

Sistemas de Gestão de Segurança da Informação

Trabalho Prático 2

FORTICLOUD

David Santos – 8220651

Fábio da Cunha – 8210619

Nuno Gomes – 8220652

ESTG, dezembro de 2024

Índice

1. Introdução

A proteção de informações sensíveis e a segurança de instalações críticas são pilares fundamentais para a gestão de segurança em qualquer organização. Este trabalho é uma continuação do primeiro estudo realizado no âmbito do Sistema de Gestão de Segurança da Informação (SGSI) da nossa empresa, que é especializada na prestação de serviços de armazenamento em nuvem e soluções de segurança informática. Enquanto o primeiro estudo focou na definição de políticas de segurança, como as Políticas de Secretária Limpa, Ecrã Limpo e controle de acessos físicos às instalações críticas, este relatório avança para etapas práticas, como a identificação de riscos, a criação de uma matriz de riscos e a elaboração da Declaração de Aplicabilidade (SOA).

A matriz de riscos, elaborada a partir da identificação de ativos críticos, como data centers, sistemas de criptografia e redes de comunicação, permite mapear cenários de vulnerabilidade que podem impactar a confidencialidade, integridade e disponibilidade das informações. Essas análises orientam a priorização de intervenções e a implementação de controles que mitiguem riscos e reforcem a resiliência dos sistemas.

Complementando essas iniciativas, a Declaração de Aplicabilidade (SOA) documenta os controles de segurança selecionados e implementados, justificando sua relevância e adequação às necessidades organizacionais. Essas medidas garantem que as diretrizes políticas sejam baseadas em evidências, estejam alinhadas às necessidades práticas e reforcem a conformidade com padrões normativos, como a ISO/IEC 27001:2022.

Além disso, as métricas e análises contidas no trabalho proporcionam uma visão detalhada sobre os controles implementados, destacando áreas de maior vulnerabilidade e níveis de conformidade observados. Combinando medidas organizacionais e operacionais, este relatório busca fortalecer a proteção dos ativos, promover uma cultura de responsabilidade e conscientização, e consolidar a confiança de nossos clientes nos serviços prestados.

2. Inventário de Ativos

A identificação de ativos é o primeiro passo para proteger os recursos críticos da organização. Nessa etapa, mapeamos os elementos essenciais, como sistemas, dados e infraestrutura, que precisam de proteção contra riscos e ameaças. Esse processo é fundamental para priorizar ações de segurança e garantir a continuidade dos serviços.

ID do Ativo	Descrição	Tipo	Proprietário	Localização
A01	Data Center Global	Infraestrutura física	Equipe de Operações	Diversos locais globais
A02	Servidores de Armazenamento em Nuvem	Equipamento físico	TI	Data Centers
A03	Sistemas de Criptografia	Software	TI	Data Centers
A04	Firewall Inteligente	Hardware/Software	Equipe de Segurança	Data Centers
A05	Plataforma de Backup	Software	TI	Nuvem
A06	Aplicações de Gestão de Identidade (IAM)	Software	TI	Infraestrutura em Nuvem
A07	Base de Dados de Clientes	Informação sensível	Equipe de Operações	Servidores em Nuvem
A08	Redes de Comunicação	Infraestrutura física	Equipe de Operações	Escritórios e Data Centers
A09	Equipes de Suporte e Operação	Recurso humano	RH	Escritórios e remoto
A10	Documentação de Políticas e Procedimentos	Informação sensível	Compliance	Servidores internos

3. Metodologia de Análise de Riscos

3.1. Introdução

A metodologia de análise de riscos aplicada foi estruturada com base nos requisitos da norma ISO 27001, integrando as etapas fundamentais de identificação, avaliação, e tratamento de riscos associados aos ativos de informação.

3.2. Etapas da Metodologia

a. Identificação de Riscos

Para cada ativo identificado, foram analisados cenários de risco associados a vulnerabilidades específicas. Esta etapa considerou:

- Possíveis eventos como perda, roubo ou falhas de infraestrutura.
- Análise de impacto em três dimensões principais: **Confidencialidade (C)**, **Integridade (I)**, e **Disponibilidade (A)**.

b. Avaliação de Riscos

A avaliação foi realizada em três etapas:

- **Impacto (I)**: Medido em uma escala de 1 a 4, representa a severidade do dano caso o risco ocorra.
- **Probabilidade (P)**: Avaliada em uma escala de 1 a 4, reflete a chance do risco se materializar.
- **Cálculo do Nível de Risco**: O risco foi calculado pela fórmula: **Nível de Risco=Impacto×Probabilidade**. Os resultados foram classificados como aceitáveis, inadmissíveis ou em zonas de atenção.

c. Aceitação do Risco

Os riscos foram categorizados de acordo com critérios pré-definidos:

- **Aceitável**: Sem necessidade de intervenção.
- **Admissível**: Intervenção de mitigação a médio prazo.
- **Inadmissível**: Intervenção de mitigação a curto prazo.
- **Crítico**: Intervenção de mitigação/eliminação imediata

d. Tratamento do Risco

Para os riscos não aceitáveis, foram atribuídas ações específicas baseadas em controlos definidos no ISO 27001 – Anexo A, como:

- Implementação de políticas (e.g., uso aceitável, segurança física).
- Mitigações técnicas (e.g., criptografia, redundância).

3.3. Responsabilidades

Para cada risco identificado, foi designado um responsável, encarregado de monitorar e implementar as ações necessárias.

4. Política de Secretária Limpa e Ecrã Limpo

4.1. Objetivo

Garantir a proteção de informações sensíveis, documentos confidenciais e ativos digitais, reduzindo o risco de acessos não autorizados, vazamentos de dados e incidentes de segurança.

4.2. Âmbito

Aplica-se a todos os colaboradores da empresa, em todos os departamentos e localizações.

4.3. Diretrizes

1. **Secretária Limpa:**
    a. Todos os documentos físicos contendo informações confidenciais ou sensíveis devem ser guardados em gavetas trancadas ou armários ao final do expediente.
    b. É proibido deixar informações confidenciais em locais visíveis, como mesas, impressoras ou áreas de uso comum.
    c. Materiais impressos não utilizados devem ser imediatamente descartados em contentores para destruição segura (ex.: triturador de papel).
2. **Ecrã Limpo:**
    a. Sempre bloqueiar o computador ou dispositivo quando estiver ausente, mesmo que seja por curtos períodos.
    b. Configurar o bloqueio automático do ecrã após 5 minutos de inatividade.
    c. Não deixar informações sensíveis visíveis no ecrã quando outras pessoas estiverem presentes.
3. **Documentos e Objetos Pessoais:**
    a. Evitar acumular itens pessoais que possam desorganizar ou desviar a atenção do cumprimento da política.
    b. Limitar o acesso a documentos e pastas apenas às pessoas autorizadas.

4.4. Monitorização e Conformidade

- A conformidade será periodicamente avaliada através de auditorias internas.
- Incidentes de não conformidade devem ser reportados à equipe de segurança da informação imediatamente.

5. Política de Acessos Físicos às Instalações Críticas

5.1. Objetivo

Proteger áreas críticas da empresa contra acessos não autorizados, assegurando a integridade dos ativos físicos e digitais da organização.

5.2. Âmbito

Esta política aplica-se a todas as instalações críticas identificadas pela empresa, como salas de servidores, arquivos confidenciais e áreas de pesquisa e desenvolvimento.

5.3. Diretrizes

1. **Controle de Acesso:**
    a. A entrada em áreas críticas será restrita a colaboradores autorizados e previamente registados.
    b. Cada colaborador autorizado deverá usar crachá de identificação visível durante sua permanência nas instalações.
    c. Todas as entradas e saídas serão monitoradas através de sistemas de controlo de acesso (ex.: cartões de acesso, biometria).
2. **Procedimentos para Visitantes:**
    a. Visitantes deverão ser previamente aprovados e acompanhados por um colaborador autorizado em todo o período de permanência.
    b. Será mantido um registo detalhado dos visitantes, incluindo nome, motivo da visita, horário de entrada e saída.
3. **Inspeção e Monitorização:**
    a. As áreas críticas deverão contar com sistemas de videovigilância 24 horas, com armazenamento seguro das gravações por, no mínimo, 30 dias.
    b. Auditorias regulares serão realizadas para garantir que os controles estão funcionando adequadamente.
4. **Resposta a Incidentes:**
    a. Qualquer tentativa de acesso não autorizado deve ser reportada à segurança imediatamente.

b. Após qualquer incidente, será feita uma revisão das permissões de acesso e implementação de melhorias, se necessário.

5.4. Treinamento e Conscientização

- Todos os colaboradores que necessitem de acesso a instalações críticas deverão participar de treinamentos periódicos sobre segurança física.

6. Considerações Finais

Este trabalho alcançou com sucesso todos os objetivos propostos para a implementação prática de um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a norma ISO/IEC 27001:2022. Desde o planejamento inicial até a execução de controles específicos, seguimos as etapas metodológicas para garantir uma abordagem robusta e alinhada com as melhores práticas de segurança da informação.

Iniciamos o projeto com a identificação e inventário dos ativos críticos da organização, passando pela análise e avaliação detalhada de riscos. Através da matriz de riscos, foi possível determinar cenários prioritários de intervenção e definir controles eficazes para mitigação e eliminação de vulnerabilidades. A Declaração de Aplicabilidade (SOA) foi construída para documentar os controles selecionados e sua relevância, estabelecendo a ligação entre a avaliação de riscos e o tratamento implementado.

Além disso, políticas específicas, como a Política de Secretária Limpa e Ecrã Limpo e a Política de Acessos Físicos às Instalações Críticas, foram desenvolvidas para abordar questões organizacionais e operacionais essenciais, fortalecendo ainda mais a proteção dos ativos e promovendo uma cultura de segurança.

Com isso, foi possível não apenas atender às exigências da norma, mas também demonstrar uma abordagem prática e estruturada para a gestão de segurança da informação, consolidando o SGSI como um pilar estratégico para a continuidade e confiança nos serviços oferecidos pela organização.