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 1

FORTICLOUD

David Santos – 8220651

Fábio da Cunha – 8210619

Nuno Gomes – 8220652

ESTG, novembro de 2024

Resumo

A FortiCloud destaca-se no setor de segurança da informação por sua infraestrutura global, equipe especializada e conformidade com regulamentações rigorosas. Este trabalho detalha o SGSI da empresa, que cobre áreas críticas como o armazenamento seguro em nuvem, defesa cibernética contra ameaças como ransomware e DDoS, e a consultoria para adequação a normas de proteção de dados, incluindo GDPR e LGPD. O trabalho inclui uma análise SWOT que identifica pontos fortes e desafios enfrentados pela FortiCloud, tais como a necessidade de investimentos contínuos em segurança e a complexidade de manter a conformidade em diferentes jurisdições. Adicionalmente, discute-se a política de segurança da informação e as estratégias de conscientização para colaboradores, o que inclui treinamentos periódicos e campanhas de sensibilização para prevenir incidentes. Através de um SGSI bem estruturado, a FortiCloud assegura o cumprimento de seus objetivos de segurança e a confiança de seus clientes.

Índice

1. Introdução

O presente trabalho aborda o desenvolvimento e implementação de um **Sistema de Gestão de Segurança da Informação (SGSI)**, com base na norma ISO 27001:2022, que visa estruturar práticas de segurança para proteger os dados e as informações estratégicas das organizações. O SGSI é essencial para mitigar riscos, assegurar conformidade regulatória e fortalecer a confiança nos processos de uma empresa. Em um contexto digital onde as ameaças cibernéticas são cada vez mais frequentes e sofisticadas, torna-se fundamental para as empresas adotar práticas robustas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade dos dados.

Neste projeto, escolhemos a empresa fictícia **FortiCloud**, que opera no setor de tecnologia e oferece soluções de armazenamento em nuvem e segurança cibernética. A FortiCloud é um exemplo relevante devido à sua atuação em áreas de alto risco, como finanças, saúde e e-commerce, onde a proteção de dados e a continuidade dos serviços são cruciais. Através de uma infraestrutura distribuída e de uma equipe especializada, a empresa aplica práticas de segurança alinhadas a normas internacionais e busca constantemente aprimorar sua resiliência contra ataques.

O conteúdo deste trabalho detalha os principais componentes de um SGSI bem estruturado, abordando aspectos como a caracterização e contexto da empresa, análise SWOT, definição de uma política de segurança da informação e estabelecimento de objetivos estratégicos para o SGSI. Além disso, são exploradas as necessidades e expectativas das partes interessadas, o escopo do sistema de gestão, a política de segurança, os controles e as práticas de conscientização. Este estudo não só demonstra a importância de um SGSI para a FortiCloud, mas também ilustra como ele pode ser implementado para atender às exigências de um mercado cada vez mais desafiador e regulamentado.

2. Caracterização da Empresa: FortiCloud

A **FortiCloud** é uma empresa de tecnologia focada em oferecer soluções robustas de **armazenamento em nuvem** e **segurança cibernética**. O nome "Forti", inspirado no *Crioulo Badiu* de Cabo Verde, significa **forte**, simbolizando a **força, resiliência e confiabilidade** dos nossos sistemas e serviços. Com sede global e uma presença marcante em mercados emergentes, a FortiCloud posiciona-se como líder na proteção e gestão de dados em ambientes digitais, atendendo clientes de diversos setores, incluindo finanças, saúde, comércio eletrônico e startups de tecnologia.

2.1. Setor de Atuação

A FortiCloud opera no **setor de serviços de cloud computing** e **segurança da informação**. A empresa fornece infraestrutura para o armazenamento de grandes volumes de dados e garante a **proteção contínua** contra ameaças cibernéticas. Além disso, oferecemos soluções de **consultoria estratégica** para empresas que precisam se adequar às regulamentações de conformidade de segurança de dados, como **ISO 27001**, **GDPR** e **HIPAA**.

2.2. Atividades Principais

- **Serviços de Armazenamento em Nuvem**: Fornecimento de serviços de *cloud computing* com alta disponibilidade, permitindo que os clientes armazenem, acessem e gerenciem grandes volumes de dados de forma segura e escalável.
- **Segurança Cibernética**: Desenvolvimento de sistemas avançados de proteção contra ameaças cibernéticas, como ataques DDoS, ransomware, malware e phishing.
- **Monitoramento e Gerenciamento de Riscos**: A FortiCloud oferece monitoramento em tempo real e gerenciamento de vulnerabilidades, detectando e respondendo a possíveis incidentes de segurança.
- **Consultoria em Conformidade Regulatória**: Auxiliamos as empresas a se adequarem às exigências de segurança da informação impostas por regulamentações internacionais.

2.3. Necessidade de Garantir a Segurança da Informação

A **segurança da informação** é fundamental para a FortiCloud, uma vez que operamos em um ambiente em que o **armazenamento seguro de dados** é a principal preocupação de nossos clientes. Empresas de **finanças**, **saúde** e **e-commerce** confiam na FortiCloud para gerenciar informações altamente sensíveis e confidenciais. A crescente sofisticação dos **ataques cibernéticos** exige que a FortiCloud mantenha um nível excepcional de **conformidade e proteção de dados**.

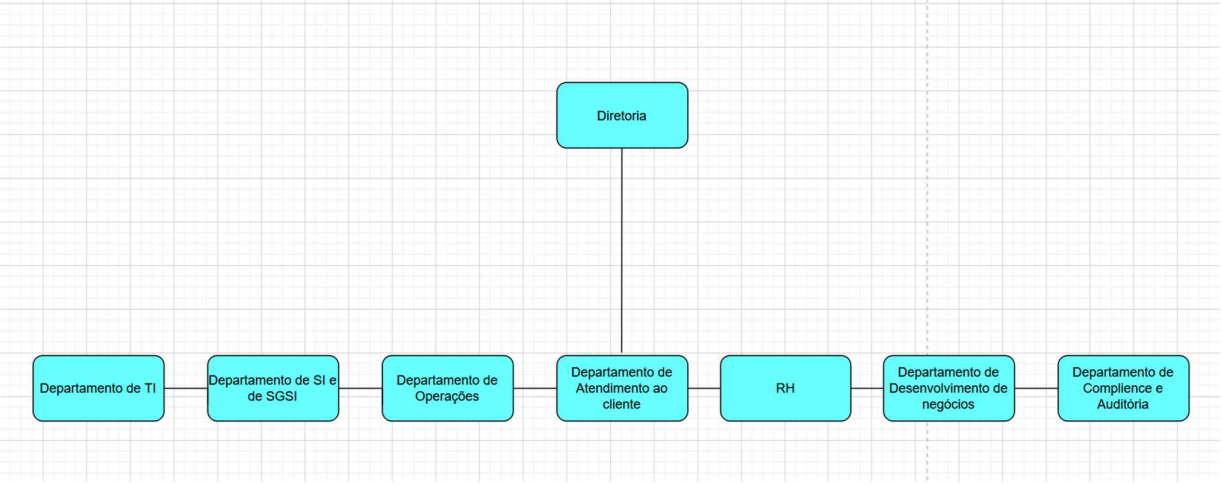
As principais necessidades de **gestão de segurança da informação (SGSI)** da FortiCloud incluem:

- **Proteção contra perda ou vazamento de dados**: A integridade dos dados de nossos clientes é primordial. Implementamos soluções de criptografia robustas para garantir que apenas indivíduos autorizados possam acessar informações sensíveis.
- **Prevenção de ataques cibernéticos**: Nosso sistema de defesa cibernética conta com tecnologias de ponta, como **firewalls inteligentes** e **sistemas de detecção de intrusão** para evitar violações de segurança.
- **Políticas de conformidade e auditoria**: Como operamos em setores regulamentados, é crucial que a FortiCloud mantenha uma política de **compliance rigorosa**, realizando auditorias periódicas para garantir a conformidade com normas como **ISO 27001:2022**.
- **Teletrabalho seguro**: Com uma equipe global, a FortiCloud adota uma política rigorosa de **segurança para o trabalho remoto**, garantindo que todos os acessos sejam feitos por meio de **VPNs** e redes seguras.

2.4. Estrutura da Empresa

A FortiCloud possui uma equipe especializada em segurança da informação, composta por analistas de segurança cibernética, engenheiros de infraestrutura de nuvem, e auditores de conformidade. Nossa infraestrutura é distribuída em vários data centers ao redor do mundo, todos operandos com os mais altos níveis de segurança e redundância.

O compromisso da FortiCloud com a segurança não é apenas um diferencial competitivo, mas uma **necessidade vital** para a confiança de nossos clientes. A implementação de um SGSI robusto, de acordo com a norma ISO 27001, fortalece nossa capacidade de proteger as informações e garantir a continuidade dos negócios de nossos clientes em um ambiente digital em constante mudança.



1. Diretoria Executiva

- Função: Definir a estratégia geral da empresa e garantir o alinhamento com os objetivos de segurança da informação e negócios.

2. Departamento de Segurança da Informação e Sistema de Gestão de Segurança de Informação

- Função: Proteger dados e sistemas da empresa.
- Responsabilidades:
    - Desenvolvimento e implementação do SGSI.
    - Monitoramento contínuo de ameaças cibernéticas.
    - Realização de auditorias de segurança e avaliações de riscos.
    - Treinamento e conscientização em segurança para todos os colaboradores.

3. Departamento de Tecnologia da Informação (TI)

- Função: Gerenciar a infraestrutura tecnológica da empresa.
- Responsabilidades:
    - Manutenção de servidores, redes e sistemas de armazenamento em nuvem.
    - Suporte técnico para funcionários e clientes.
    - Implementação de soluções de software e hardware.

4. Departamento de Operações

- Função: Garantir a eficiência dos serviços oferecidos pela FortiCloud.
- Responsabilidades:
    - Gerenciamento do data center e recursos de nuvem.
    - Garantia de uptime e continuidade dos serviços.
    - Monitoramento de desempenho e capacidade de recursos.

5. Departamento de Atendimento ao Cliente

- Função: Fornecer suporte e assistência a clientes.
- Responsabilidades:
    - Resolução de problemas e dúvidas dos clientes.
    - Treinamento de clientes sobre o uso dos serviços da FortiCloud.
    - Coleta de feedback para melhoria dos serviços.

6. Departamento de Desenvolvimento de Negócios

- Função: Expandir a base de clientes e parcerias.
- Responsabilidades:
    - Identificação de novas oportunidades de mercado.
    - Desenvolvimento de estratégias de marketing e vendas.
    - Estabelecimento de parcerias estratégicas com outras empresas.

7. Departamento de Compliance e Auditoria

- Função: Garantir que a empresa atenda a todas as regulamentações de segurança da informação.
- Responsabilidades:
    - Realização de auditorias internas e externas.
    - Monitoramento de conformidade com normas como ISO 27001 e GDPR.
    - Atualização de políticas e procedimentos conforme novas regulamentações.

8. Departamento de Recursos Humanos

- Função: Gerenciar o capital humano da empresa.
- Responsabilidades:
    - Recrutamento e seleção de pessoal qualificado.
    - Treinamento e desenvolvimento de funcionários.
    - Gestão de políticas internas de segurança e ética.

3. Análise SWOT da FortiCloud

3.1. Forças (Strengths)

- **Infraestrutura Tecnológica Global e Resiliente:** A FortiCloud conta com data centers distribuídos globalmente, garantindo alta disponibilidade, redundância e proteção contra falhas e incidentes.
- **Equipe Especializada:** Possui uma equipe técnica qualificada em áreas como segurança cibernética, infraestrutura em nuvem e conformidade, garantindo excelência na operação e segurança.
- **Conformidade com Normas Internacionais:** A empresa está em conformidade com regulamentações como ISO 27001 e GDPR, essencial para atrair clientes dos mais diversos setores.

- **Soluções de Segurança Avançadas:** Utilização de *firewalls* inteligentes, criptografia e sistemas de deteção de intrusão, proporcionando uma proteção robusta contra ameaças cibernéticas, como *ransomware* e ataques *DDoS*.
- **Cultura de Conscientização em Segurança:** A FortiCloud promove programas contínuos de treinamento e conscientização para seus colaboradores, criando um ambiente focado em boas práticas de segurança.

3.2. Fraquezas (Weaknesses)

- **Custo Elevado de Implementação e Manutenção de SGSI:** A necessidade de investimentos contínuos em infraestrutura, auditorias e atualizações pode ser onerosa e afetar a rentabilidade.
- **Complexidade de Gerenciamento de Conformidade Multi-jurisdicional:** Manter a conformidade com diferentes regulamentações de segurança em múltiplos mercados (por exemplo, GDPR na Europa e HIPAA nos EUA) pode ser complexo e caro.
- **Dependência de Fornecedores de Terceiros:** O uso de soluções de terceiros pode expor a FortiCloud a riscos de segurança externos que não estão sob seu controle direto.
- **Sobrecarga da Equipe de Segurança:** A equipe de segurança pode ser pressionada pelo grande volume de alertas e incidentes cibernéticos, exigindo uma resposta ágil e eficiente.
- **Desafios de Teletrabalho Seguro:** Manter a segurança no trabalho remoto em uma equipe global apresenta desafios em termos de consistência na implementação de políticas e controle de acessos.

3.3. Oportunidades (Opportunities)

- **Crescimento da Demanda por Serviços de Cloud e Segurança:** Com a digitalização global e o aumento do trabalho remoto, a demanda por serviços de armazenamento em nuvem seguros e proteção de dados está em alta.
- **Inovação em Tecnologias de Segurança:** A adoção de tecnologias emergentes, como inteligência artificial e machine learning, para detecção automática de ameaças oferece uma oportunidade de fortalecer ainda mais o SGSI.
- **Parcerias Estratégicas:** Parcerias com outras empresas de segurança cibernética podem trazer tecnologias inovadoras e permitir a ampliação de mercados.
- **Serviços de Consultoria em Segurança da Informação:** A FortiCloud pode expandir oferecendo consultoria especializada para outras empresas que precisam implementar SGSI, especialmente em mercados emergentes.

3.4. Ameaças (Threats)

- **Aumento nas Ameaças Cibernéticas:** O crescimento de ataques cibernéticos sofisticados, como *ransomware*, pode colocar a FortiCloud e seus clientes em risco, exigindo defesas mais robustas.
- **Mudanças nas Regulamentações:** Alterações nas leis de privacidade e segurança de dados, como o GDPR, podem exigir adaptações frequentes, aumentando os custos de conformidade.
- **Concorrência Agressiva:** Empresas maiores ou mais inovadoras no mercado de nuvem e segurança cibernética podem atrair clientes da FortiCloud oferecendo tecnologias mais avançadas ou preços mais competitivos.
- **Riscos Associados a Terceirização:** A dependência de fornecedores terceirizados pode introduzir falhas de segurança ou comprometer a resiliência do SGSI da FortiCloud.
- **Quebra de Confiança por Violações de Dados:** Um incidente grave de violação de dados pode prejudicar a reputação da empresa e levar a perdas financeiras e legais significativas.

4. Determinação das Necessidades e Expectativas das Partes Interessadas

Para a FortiCloud, a identificação das partes interessadas é fundamental para garantir que as políticas e práticas de segurança da informação atendam às suas necessidades e expectativas. A seguir, estão as principais partes interessadas e suas expectativas em relação à segurança da informação (SI), além das exigências legais que influenciam o SGSI da empresa.

4.1. Identificação das Partes Interessadas

I. **Clientes**:

- Empresas dos setores de **finanças**, **saúde**, **e-commerce**, e **startups tecnológicas**, que dependem de serviços de **cloud computing** e **segurança de dados** oferecidos pela FortiCloud.

II. **Colaboradores**:

- **Funcionários e prestadores de serviços** da FortiCloud, especialmente aqueles que trabalham em funções críticas de **desenvolvimento de software**, **infraestrutura em nuvem** e **segurança cibernética**.

III. **Fornecedores**:

- **Provedores de tecnologia**, **fabricantes de hardware**, e **fornecedores de soluções de segurança** que oferecem as ferramentas e infraestruturas usadas pela FortiCloud.

IV. **Órgãos Reguladores**:

- **Entidades governamentais e reguladoras**, como **Comissões de Proteção de Dados** (no caso do GDPR) e órgãos responsáveis por regulamentar a **segurança cibernética e privacidade de dados**, que supervisionam o cumprimento das normas e regulamentações.

V. **Acionistas e Investidores**:

- **Investidores** da FortiCloud que esperam **crescimento sustentável** e **conformidade** com padrões de segurança da informação para proteger a reputação e garantir a viabilidade da empresa.

VI. **Parceiros e Consultorias de Segurança**:

- **Empresas parceiras** especializadas em tecnologias complementares que colaboram com a FortiCloud para aprimorar suas ofertas de segurança.

4.2. Principais Expectativas em Relação à Segurança da Informação

I. **Clientes**:

- **Proteção de dados confidenciais**: Esperam que a FortiCloud garanta a integridade, confidencialidade e disponibilidade de suas informações sensíveis, incluindo dados financeiros, informações médicas e segredos industriais.
- **Continuidade de serviço**: Garantir **alta disponibilidade** dos serviços de nuvem, com **recuperação rápida de desastres** e **proteção contra ataques cibernéticos**.
- **Conformidade com regulamentações**: Clientes dos setores regulados, como saúde e finanças, exigem que a FortiCloud cumpra normas como **ISO 27001**, **GDPR**, entre outras.

II. **Colaboradores**:

- **Ambiente de trabalho seguro**: Acesso seguro aos sistemas internos, especialmente para equipes remotas, por meio de **VPNs** e **autenticação multifatorial**.
- **Treinamento e conscientização**: Os colaboradores esperam estar **bem informados e treinados** sobre as melhores práticas de segurança e suas responsabilidades em relação à proteção de dados.

III. **Fornecedores**:

- **Parcerias seguras**: Fornecedores de tecnologia esperam que a FortiCloud adote políticas claras de **gestão de fornecedores**, garantindo que seus produtos e serviços não comprometam a segurança da informação.
- **Processos de integração seguros**: Exigem uma **colaboração transparente e segura**, especialmente na troca de dados e soluções tecnológicas.

IV. **Órgãos Reguladores**:

- **Conformidade total com a legislação**: Os reguladores esperam que a FortiCloud cumpra rigorosamente todas as **normas de segurança e privacidade** de dados aplicáveis.
- **Auditorias regulares**: A FortiCloud deve estar preparada para **auditorias de conformidade**, comprovando que os controles de segurança estão adequados e que há **gestão eficaz de riscos**.

V. **Acionistas e Investidores**:

- **Minimização de riscos financeiros**: Esperam que a empresa **mitigue os riscos de violações de dados** que poderiam impactar negativamente o valor da empresa ou resultar em **sanções legais**.
- **Conformidade contínua**: Acionistas exigem que a FortiCloud permaneça em conformidade com as regulamentações para evitar perdas financeiras, processos legais e danos à reputação.

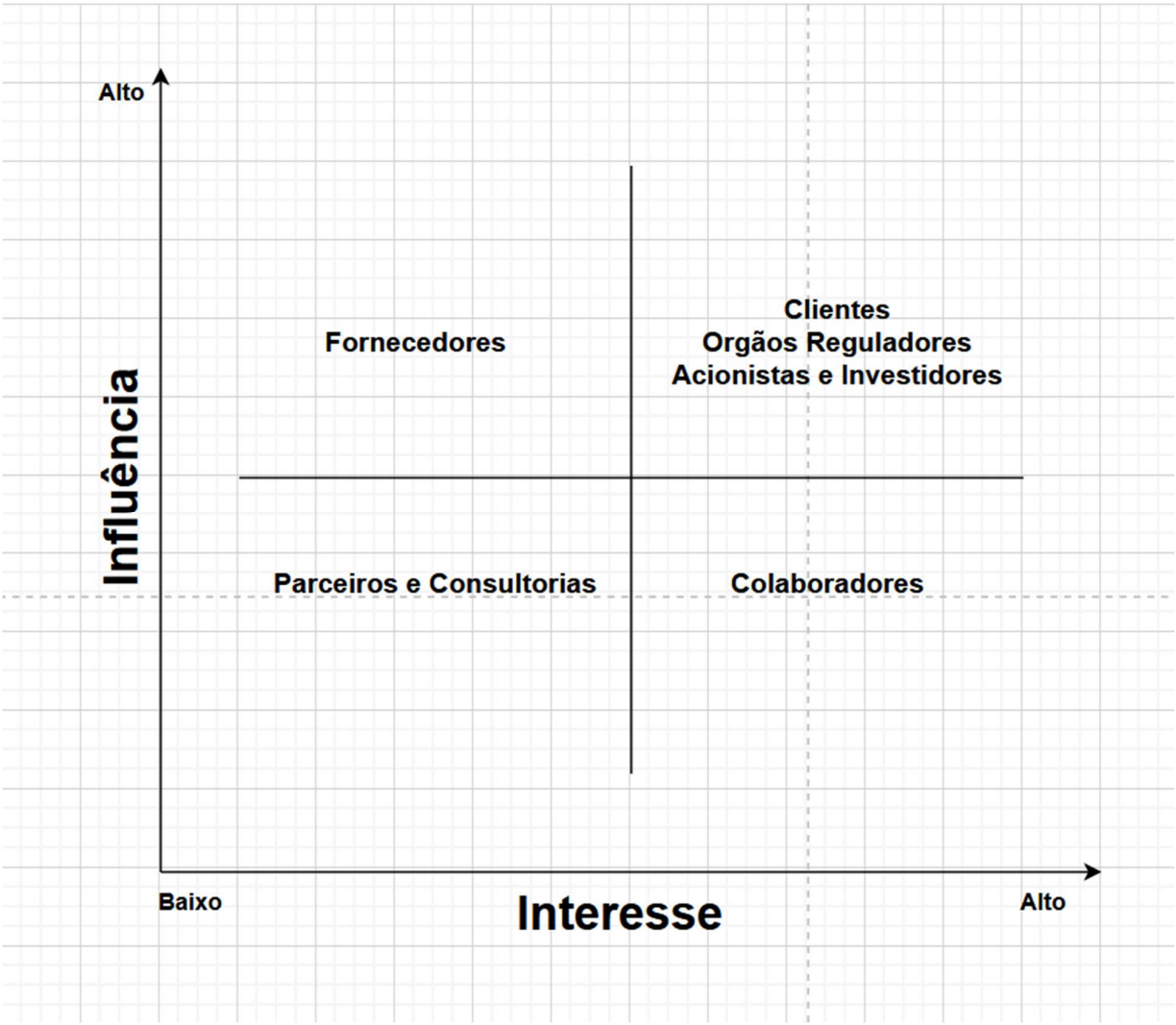
VI. **Parceiros e Consultorias**:

- **Interoperabilidade e segurança**: Parceiros esperam que as integrações entre as soluções sejam **seguras**, sem expor sistemas a vulnerabilidades.

4.3. Exigências Legais e Regulamentares que Afetam a Segurança da Informação

1. **ISO 27001**:
   - A FortiCloud segue o **SGSI** alinhado à norma **ISO 27001**, garantindo a **gestão de riscos** de segurança da informação e a **implementação de controles** adequados.
2. **GDPR (Regulamento Geral sobre a Proteção de Dados)**:
   - A FortiCloud deve garantir a **proteção de dados pessoais** de cidadãos da União Europeia, respeitando os direitos de privacidade e notificando incidentes de segurança dentro do prazo legal.
3. **HIPAA (Health Insurance Portability and Accountability Act)**:
   - Para clientes do setor de saúde nos EUA, a FortiCloud deve garantir a **proteção de informações de saúde eletrônica**, seguindo os padrões da HIPAA.
4. **Lei Geral de Proteção de Dados (LGPD)**:
   - A FortiCloud também deve se adequar às regulamentações de **proteção de dados no Brasil**, garantindo a privacidade dos dados pessoais em conformidade com a **LGPD**.

4.4. Matriz dos StakeHolders da FortiCloud



Alto Interesse e Alta Influência:

- **Clientes**: Exigem altos níveis de segurança e continuidade de serviço.
- **Órgãos Reguladores**: Demandam conformidade total com normas de proteção de dados e segurança.
- **Acionistas e Investidores**: Esperam mitigação de riscos e conformidade contínua para proteger o valor e a reputação da empresa.

Alta Influência e Baixo Interesse:

- **Fornecedores**: Precisam de políticas de segurança claras para parcerias, mas não se envolvem diretamente em operações do SGSI.

Baixa Influência e Baixo Interesse:

- **Parceiros e Consultorias**: Interesse em segurança para interoperabilidade, porém com baixa influência direta sobre o SGSI.

Baixa Influência e Alto Interesse:

- **Colaboradores**: Têm interesse em um ambiente seguro e em treinamentos contínuos, mas baixa influência sobre as decisões do SGSI.

5. Âmbito do Sistema de Gestão de Segurança da Informação (SGSI)

O **Sistema de Gestão de Segurança da Informação (SGSI)** da FortiCloud abrange todas as áreas críticas e processos relacionados à segurança da informação, conforme os serviços oferecidos pela empresa. O objetivo do SGSI é garantir a **proteção, confidencialidade, integridade e disponibilidade** das informações geridas pela FortiCloud, tanto para seus clientes quanto para suas operações internas.

5.1. Escopo do SGSI

O SGSI da FortiCloud cobre as seguintes áreas e serviços:

I. **Serviços de Armazenamento em Nuvem**:

- **Infraestrutura de cloud computing**: Inclui os **data centers globais**, os sistemas de armazenamento e os processos de backup e recuperação de desastres. Este é um componente fundamental do SGSI, uma vez que a FortiCloud garante a **alta disponibilidade e escalabilidade** do armazenamento seguro de dados.
- **Acesso e gestão de dados**: O controle de acesso e a **criptografia de dados** em repouso e em trânsito são parte central do SGSI, garantindo que os dados dos clientes estejam protegidos contra acessos não autorizados.

II. **Segurança Cibernética**:

- **Sistemas de defesa cibernética**: O SGSI abrange os processos de **proteção contra ataques cibernéticos**, incluindo **DDoS, ransomware, malware e phishing**. Isso inclui a implementação de **firewalls inteligentes, sistemas de detecção de intrusão (IDS)** e **tecnologias de criptografia**.
- **Resposta a incidentes de segurança**: O sistema de resposta rápida a incidentes está incluído no SGSI, garantindo que todas as ameaças e vulnerabilidades identificadas sejam resolvidas rapidamente.

III. **Monitoramento e Gerenciamento de Riscos**:

- **Monitoramento contínuo**: Os serviços de **monitoramento em tempo real** e **gerenciamento de vulnerabilidades** estão dentro do escopo, garantindo a **detecção de incidentes** e a resposta proativa a **riscos de segurança**.
- **Avaliações de risco periódicas**: A FortiCloud realiza **avaliações de risco** regulares em todos os seus sistemas e serviços, o que é parte integral do SGSI, com o objetivo de identificar e mitigar novos riscos à segurança da informação.

IV. **Consultoria em Conformidade Regulatória**:

- **Serviços de consultoria de conformidade**: Os processos que auxiliam os clientes a atender às regulamentações de segurança da informação (como **ISO 27001, GDPR, HIPAA, LGPD**) estão dentro do escopo do SGSI, garantindo que as soluções de segurança oferecidas estejam em conformidade com as exigências legais.
- **Relatórios e auditorias**: A geração de **relatórios de conformidade** e a **realização de auditorias internas e externas** também fazem parte do SGSI, assegurando que a FortiCloud e seus clientes estejam sempre em conformidade com as normas aplicáveis.

V. **Ambiente de trabalho e teletrabalho seguro**:

- O SGSI cobre os processos de **segurança no acesso remoto**, incluindo o uso de **VPNs, autenticação multifator** e a gestão de acessos dos colaboradores que trabalham remotamente.
- **Segurança física** dos locais onde os **data centers** estão situados, incluindo **controles de acesso físico** e monitoramento de vigilância.

5.2. Exclusões do SGSI

1. **Sistemas e processos internos administrativos**: O SGSI da FortiCloud não inclui sistemas puramente **administrativos** (por exemplo, sistemas de contabilidade interna, folha de pagamento), a menos que estejam diretamente relacionados com a segurança da informação ou integrem processos críticos de TI.
    - **Justificativa**: Esses sistemas não afetam diretamente os serviços oferecidos aos clientes e são gerenciados por políticas de segurança específicas para operações administrativas.
2. **Soluções de terceiros não gerenciadas diretamente pela FortiCloud**: O SGSI não cobre soluções de terceiros usadas por clientes fora do ambiente gerenciado pela FortiCloud.
    - **Justificativa**: A FortiCloud oferece suporte para segurança da informação, mas as soluções externas implementadas pelos clientes fora de nossa infraestrutura estão fora de nosso controle direto.

6. Política de Segurança da informação

O desenvolvimento de uma Política de Segurança da Informação (SI) para FortiCloud, que fornece maioritariamente serviços de nuvem, é uma ação crucial para proteger tanto os dados sensíveis de clientes quanto as operações internas da empresa. A política deve abordar princípios, procedimentos e controles de segurança, levando em consideração a natureza dos serviços em nuvem e garantindo os princípios de privacidade, confidencialidade, integridade e disponibilidade de dados.

6.1. Objetivo

- **Objetivo da Política**: Estabelecer diretrizes para garantir a proteção e segurança dos dados armazenados, processados e transmitidos por meio dos serviços em nuvem oferecidos pela FortiCloud.
- **Abrangência**: Definir que a política se aplica a todos os colaboradores, prestadores de serviço, fornecedores e quaisquer outras partes que tenham acesso à infraestrutura e aos dados da empresa.

6.2. Normas e Regulamentações

- **Conformidade Legal**: A política deve estar alinhada com regulamentações e normas vigentes, como a **ISO 27001**, **GDPR** (para clientes da UE) e **LGPD** no Brasil.
- **Padrões de Segurança**: Incorporar boas práticas de frameworks de segurança como **NIST** (National Institute of Standards and Technology), ou o **CIS Controls** para segurança de TI.

6.3. Controle de Acesso e Identidade

- **Gerenciamento de Acesso**: Implementar uma política de controle de acesso que permita apenas a utilizadors autorizados o acesso aos sistemas e dados sensíveis. Isso inclui o uso de autenticação de dois fatores (2FA), políticas de senha forte e o conceito de **least privilege** (privilégio mínimo).
- **Gerenciamento de Identidade**: Utilizar ferramentas de **IAM (Identity Access Management)** para gerenciar identidades digitais e controlar o acesso de utilizadors aos serviços em nuvem.

6.4. Classificação e Proteção de Dados

- **Classificação de Dados**: Definir um esquema de classificação de dados (por exemplo, Público, Confidencial, Secreto) e aplicar controles adequados com base na sensibilidade dos dados.
- **Criptografia**: Implementar criptografia de ponta a ponta para dados em trânsito e em repouso. Isso garantirá que os dados estejam protegidos, mesmo se houver violação de segurança.

6.5. Segurança na Nuvem

- **Responsabilidades Compartilhadas**: Deixar claro o modelo de responsabilidade compartilhada entre a FortiCloud e os provedores de serviços de nuvem (como AWS, Azure, Google Cloud), incluindo segurança da infraestrutura e do conteúdo armazenado.
- **Monitoração e Auditoria**: Implementar sistemas de monitoração contínua para detecção de ameaças, vulnerabilidades e atividades anômalas. Registar logs de acesso e atividades importantes para auditorias futuras.
- **Backup e Recuperação de Desastres**: Definir e aplicar estratégias de backup frequente dos dados, com testes regulares de recuperação para garantir continuidade do negócio em caso de incidentes.

6.6. Proteção Contra Ameaças e Incidentes

- **Prevenção e Resposta a Incidentes**: Definir procedimentos para resposta a incidentes de segurança, incluindo a formação de um **CSIRT (Computer Security Incident Response Team)**. Ter um plano claro de comunicação e mitigação em caso de vazamento ou violação de dados.
- **Treinamento de Segurança**: Proporcionar treinamento regular para funcionários e colaboradores sobre boas práticas de segurança da informação, phishing, engenharia social e outros vetores de ataque.

6.7. Gestão de Vulnerabilidades e Atualizações

- **Atualizações e Patches**: Garantir que todos os sistemas, serviços e dispositivos conectados estejam sempre atualizados com os últimos patches de segurança.
- **Testes de Penetração**: Realizar regularmente testes de penetração (pentests) e auditorias para identificar vulnerabilidades e melhorar os sistemas de defesa.

6.8. Gerenciamento de Terceiros e Fornecedores

- **Avaliação de Segurança**: Avaliar a segurança dos fornecedores de serviços em nuvem e de outros parceiros externos, garantindo que eles atendam aos mesmos padrões de segurança adotados pela FortiCloud.
- **Acordos de Confidencialidade (NDA)**: Exigir a assinatura de NDAs para colaboradores, prestadores de serviço e fornecedores, garantindo a proteção de informações confidenciais.

6.9. Políticas de Privacidade e Gestão de Dados Pessoais

- **Gestão de Dados Pessoais**: Garantir o cumprimento das legislações de proteção de dados (como LGPD e GDPR) e criar processos para gerenciamento seguro de dados pessoais.
- **Direitos do Titular dos Dados**: Estabelecer processos para que os titulares dos dados possam exercer seus direitos, como acesso, correção, portabilidade e exclusão de dados, conforme exigido por lei.

6.10. Revisão e Atualização da Política

- **Auditorias Internas**: Programar auditorias periódicas para revisar a efetividade das medidas de segurança adotadas.
- **Atualizações**: Manter a política atualizada para incorporar novos riscos, regulamentações ou mudanças tecnológicas. É recomendado revisar a política anualmente ou em caso de grandes mudanças no ambiente de TI.

7. Política de Comunicação e Classificação de Informação

Para gerenciar adequadamente o acesso e a proteção de informações, a FortiCloud deve ter uma **política de classificação de dados/informação documentada**, que define os requisitos para cada tipo de dado (Público, Confidencial e Secreto).

7.1. Propósito e Escopo

Estabelecer diretrizes e normas para a classificação e proteção de dados, com o objetivo de garantir a segurança das informações, respeitar a privacidade de clientes e colaboradores e mitigar riscos para a empresa.

Aplica-se a todos os dados gerenciados pela FortiCloud, incluindo documentos físicos e digitais, e abrange todos os funcionários, prestadores de serviço e parceiros de negócios.

7.2. Definições de Classificação

- **Público**: Dados acessíveis ao público em geral, sem risco de impacto negativo à empresa ou aos clientes. Não contêm informações sensíveis e requerem controle mínimo.
- **Confidencial**: Dados sensíveis, cujo acesso é restrito a colaboradores autorizados e parceiros com necessidade de saber. Exposição destes dados pode gerar impacto moderado na reputação ou operações da empresa.
- **Secreto**: Dados altamente sensíveis que exigem o mais alto nível de proteção, pois sua exposição pode causar sérios danos financeiros, reputacionais e legais à empresa. Apenas pessoal essencial pode acessá-los.

7.3. Regras de Classificação e Controle

- **Classificação de Novos Dados**: Todos os dados criados ou recebidos pela FortiCloud devem ser classificados de acordo com as diretrizes e revisados periodicamente.
- **Reclassificação**: Sempre que houver alteração na sensibilidade dos dados, eles devem ser reclassificados e aplicados os controles apropriados.

- **Responsabilidade pela Classificação**: O responsável pelo dado (dono da informação) deve garantir a classificação correta e monitorar os acessos.

7.4. Controles e Requisitos para Cada Nível

1. **Dados Públicos**:
    a. Podem ser compartilhados externamente sem controle adicional.
    b. Armazenamento em áreas de acesso geral, monitorado para prevenir modificações não autorizadas.
2. **Dados Confidenciais**:
    a. Criptografia obrigatória para dados em repouso e em trânsito.
    b. Acesso restrito a colaboradores autorizados, com monitoramento de atividade.
    c. Regras de armazenamento seguro (servidores internos e seguros).
    d. Proibição de compartilhamento externo sem autorização formal.
3. **Dados Secretos**:
    a. Criptografia avançada e segmentação de rede.
    b. Autenticação multifatorial (MFA) e controle de acesso restrito.
    c. Revisões regulares de acesso e auditoria de uso.
    d. Proibição estrita de impressão, cópia ou exportação sem autorização explícita.

7.5. Gerenciamento e Monitoramento de Conformidade

- **Auditorias Periódicas**: A equipe de compliance deve realizar auditorias regulares para garantir que as classificações e controles estão sendo aplicados corretamente.
- **Treinamento e Conscientização**: Todos os colaboradores devem participar de treinamentos periódicos sobre a política de classificação de dados.
- **Relatórios e Incidentes**: Incidentes de segurança devem ser documentados e analisados, e relatórios periódicos devem ser gerados para revisar a eficácia da política.

7.6. Penalidades e Consequências

Colaboradores que violarem as políticas de classificação e proteção de dados podem estar sujeitos a medidas disciplinares, incluindo demissão, além de consequências legais, dependendo da gravidade da violação.

8. Objetivos Estratégicos de Segurança da Informação

Objetivo Global	Processo	Ações para cumprimento dos Objetivos Globais	Resp	Prazo	Indicadores de Medida	Meta	Acompanhamento
Melhorar a Proteção contra Ameaças Cibernéticas	Conceção, execução, qualidade, cliente	- Implementar sistemas avançados de deteção de intrusões (IDS/IPS). - Revisar e atualizar políticas de firewall e anti-malware. - Aplicar patches de segurança regularmente.	Equipe de TI	12 meses	Número de incidentes de segurança detectados por sistemas de monitoramento	Reduzir incidentes em 60%	Revisões trimestrais
Garantir a Conformidade com Leis e Regulamentações	Concepção, execução, cliente	- Auditar conforme GDPR e outras regulamentações. - Implementar um sistema de controle de acesso baseado em funções (RBAC). - Assegurar a coleta de consentimento dos dados.	Equipe de Compliance	6 meses	Percentual de conformidade nas auditorias de segurança	Atingir 100% de conformidade em auditorias externas	Auditoria semestral
Aumentar a Conscientização dos Colaboradores	Conceção, execução	- Oferecer treinamento contínuo sobre melhores práticas de segurança cibernética. - Realizar campanhas de phishing.	Recursos Humanos e TI	6 meses	Percentual de conformidade nas auditorias de segurança	Atingir 100% de conformidade em auditorias externas	Avaliação trimestral dos resultados
Implementar Controles Efetivos para Minimizar Riscos	Conceção, qualidade	- Identificar e priorizar riscos em uma matriz de risco. - Implementar controle de acesso físico e lógico mais rígido. - Revisar e testar os planos de resposta a incidentes.	Recursos Humanos e TI	12 meses	Número de falhas de segurança relacionadas a riscos identificados	Reduzir falhas em 50%	Monitoramento contínuo e revisão anual

8.1. Melhorar a Proteção contra Ameaças Cibernéticas

Processo: Conceção, execução, qualidade, cliente.

Ações para cumprimento:

- Implementar sistemas avançados de deteção de intrusões (IDS/IPS).
- Revisar e atualizar políticas de firewall e anti-malware.
- Aplicar patches de segurança regularmente.

Responsáveis: Equipe de TI

Prazo: 12 meses

Indicadores de Medida:

- Número de incidentes de segurança detetados por sistemas de monitoramento.

Meta: Reduzir incidentes em 60%.

Acompanhamento: Revisões trimestrais.

8.2. Garantir a Conformidade com Leis e Regulamentações

Processo: Qualidade, execução, cliente.

Ações para cumprimento:

- Auditar regularmente a conformidade com GDPR e outras regulamentações aplicáveis.
- Implementar um sistema de controle de acesso baseado em funções para garantir o acesso adequado.
- Assegurar a coleta de consentimento dos dados conforme as leis.

Responsáveis: Equipe de Compliance.

Prazo: 6 meses

Indicadores de Medida:

- Percentual de conformidade nas auditorias de segurança.

Meta: Atingir 100% de conformidade em auditorias externas.

Acompanhamento: Auditoria semestral.

8.3. Aumentar a Conscientização dos Colaboradores

Processo: Conceção, execução.

Ações para cumprimento:

- Oferecer treinamento contínuo sobre melhores práticas de segurança cibernética.
- Realizar campanhas de phishing simuladas para reforçar a vigilância dos colaboradores.

Responsáveis: Recursos Humanos e TI

Prazo: 6 meses

Indicadores de Medida:

- Percentual de participação em treinamentos e índice de sucesso nas simulações de phishing.

Meta: 90% de participação e sucesso nas simulações.

Acompanhamento: Avaliação trimestral dos resultados.

8.4. Implementar Controles Efetivos para Minimizar Riscos

Processo: Concepção, qualidade.

Ações para cumprimento:

- Identificar e priorizar riscos em uma matriz de risco.
- Implementar controle de acesso físico e lógico mais rígido.
- Revisar e testar os planos de resposta a incidentes.

Responsáveis: Equipe de Segurança

Prazo: 12 meses

Indicadores de Medida:

- Número de falhas de segurança relacionadas a riscos identificados.

Meta: Reduzir falhas em 50%.

Acompanhamento: Monitoramento contínuo e revisão anual.

9. Política de Passwords

9.1. Objetivo

Estabelecer normas para a criação, uso e gerenciamento seguro de senhas, garantindo que todos os utilizadors da FortiCloud utilizem senhas robustas e seguras, protegendo o acesso aos sistemas e dados sensíveis.

9.2. Abrangência

Esta política se aplica a todos os colaboradores, fornecedores e prestadores de serviço que utilizam sistemas, plataformas ou serviços controlados pela FortiCloud.

9.3. Requisitos de Complexidade das Senhas

As senhas devem atender aos seguintes critérios mínimos:

- Comprimento mínimo: 12 caracteres.
- **Variedade de caracteres**: Devem conter pelo menos:
- Uma letra maiúscula (A-Z),
- Uma letra minúscula (a-z),
- Um número (0-9),
- Um caractere especial (ex.: @, #, $, %).
- **Proibição de senhas comuns**: Senhas como "123456", "senha", "admin", ou variações semelhantes são proibidas.
- **Evitar dados pessoais**: Senhas não devem conter informações pessoais facilmente identificáveis, como nomes, datas de nascimento ou números de identificação.

9.4. Frequência de Troca de Senhas

- As senhas devem ser alteradas **a cada 90 dias**.
- Em caso de suspeita de comprometimento, a senha deve ser alterada imediatamente.

9.5. Gerenciamento de Senhas

- **Autenticação Multifator (MFA)**: Além da senha, o uso de autenticação de dois fatores (2FA) é obrigatório para acessar sistemas críticos ou dados sensíveis.
- **Armazenamento de Senhas**: As senhas nunca devem ser escritas em papéis, enviadas por e-mail ou armazenadas em locais inseguros. Os utilizadors devem usar gerenciadores de senhas confiáveis para o armazenamento seguro.
- **Histórico de Senhas**: Não é permitido reutilizar as últimas 5 senhas.

9.6. Bloqueio de Conta

- Após **5 tentativas falhas de login**, a conta será bloqueada automaticamente por 30 minutos ou até ser desbloqueada pelo administrador de sistemas.

9.7. Senhas Temporárias

- Senhas temporárias geradas para novos utilizadors ou para recuperação de conta devem ser alteradas no primeiro login.

9.8. Responsabilidades dos Utilizadores

- **Confidencialidade**: Cada utilizador é responsável por manter a confidencialidade de sua senha. O compartilhamento de senhas é estritamente proibido.
- **Uso Adequado**: As senhas devem ser usadas apenas para aceder a sistemas autorizados e conforme a necessidade de trabalho.

10. Política de Teletrabalho

10.1. Objetivo

Estabelecer diretrizes para o trabalho remoto (teletrabalho) na FortiCloud, assegurando a proteção dos sistemas de TI e dos dados corporativos, mesmo quando os colaboradores não estão no escritório.

10.2. Abrangência

Esta política se aplica a todos os colaboradores e contratados que realizam atividades profissionais remotamente, utilizando dispositivos próprios ou fornecidos pela empresa para acessar sistemas e dados corporativos.

10.3. Requisitos para o Ambiente de Trabalho Remoto

- **Espaço Adequado**: O colaborador deve assegurar que seu local de trabalho remoto seja privado e adequado, sem riscos de interrupção por terceiros.
- **Proteção de Dados**: Em caso de trabalhos em ambientes compartilhados ou públicos, é obrigatório o uso de telas de privacidade e o cuidado para evitar exposição indevida de dados sensíveis.

10.4. Segurança dos Dispositivos

- **Dispositivos da Empresa**: Sempre que possível, o colaborador deve utilizar dispositivos fornecidos pela FortiCloud, devidamente configurados com as políticas de segurança da empresa.
- **Dispositivos Pessoais**: Se for necessário utilizar dispositivos pessoais, eles devem estar em conformidade com as seguintes exigências:
    - Atualizações de sistema operacional e software de segurança em dia,
    - Instalação de software antivírus atualizado,
    - Bloqueio de tela automático após período de inatividade (máximo de 10 minutos).

10.5. Acesso Remoto Seguro

- **VPN Obrigatória**: Todo acesso remoto aos sistemas da FortiCloud deve ser realizado por meio de uma **rede VPN** (Virtual Private Network) fornecida pela empresa, garantindo uma comunicação segura e criptografada.
- **Autenticação Multifator (MFA)**: O uso de 2FA é obrigatório para acessar sistemas e recursos corporativos remotamente.

10.6. Conectividade de Rede

- **Redes Wi-Fi Seguras**: O colaborador deve garantir que a rede Wi-Fi utilizada no teletrabalho esteja devidamente protegida com senha forte e criptografia WPA3 (ou, no mínimo, WPA2).
- **Proibição de Redes Públicas**: É estritamente proibido aceder a sistemas corporativos de redes Wi-Fi públicas ou abertas (ex.: cafeterias, aeroportos, etc.).

10.7. Gerenciamento de Dados e Confidencialidade

- **Armazenamento de Dados**: Todos os dados sensíveis ou confidenciais devem ser armazenados na infraestrutura de nuvem da empresa e não em dispositivos locais.
- **Transferência de Dados**: A transferência de dados sensíveis para dispositivos externos ou serviços de armazenamento pessoal é estritamente proibida.
- **Descarte de Informações**: Impressões de documentos confidenciais em casa devem ser evitadas. Caso necessário, esses documentos devem ser descartados de forma segura (ex.: triturados).

10.8. Política de Backup

- **Backup Automático**: Todos os dados trabalhados remotamente devem ser armazenados em soluções de backup automático integradas aos sistemas de nuvem da FortiCloud, garantindo que nenhuma informação seja perdida em caso de falha do dispositivo remoto.

10.9. Responsabilidades do Colaborador

- **Segurança Física**: O colaborador é responsável por garantir a segurança física de seus dispositivos, evitando furtos ou perdas.
- **Relato de Incidentes**: Qualquer incidente de segurança, como perda de dispositivo ou atividade suspeita, deve ser reportado imediatamente ao departamento de TI.

10.10. Monitoramento e Auditoria

A FortiCloud se reserva o direito de monitorar, mediante aviso, as atividades realizadas em dispositivos corporativos e acesso remoto para garantir o cumprimento desta política.

10.11. Treinamento e Conscientização

Todos os colaboradores que realizam teletrabalho devem participar de treinamentos periódicos sobre boas práticas de segurança no trabalho remoto, incluindo prevenção contra ataques de phishing e engenharia social.

11. Campanha de Sensibilização em Segurança da Informação

11.1. Importância da Campanha

A segurança da informação é fundamental para proteger dados sensíveis e garantir a integridade dos sistemas na FortiCloud. Com o aumento das ameaças cibernéticas, é essencial que todos os colaboradores estejam cientes das práticas de segurança, dos riscos envolvidos e da importância de manter um ambiente digital seguro. Esta campanha visa criar uma cultura de segurança robusta, onde cada colaborador entende e assume a responsabilidade pela proteção das informações da empresa.

11.2. Objetivos da Campanha

Aumentar a Conscientização: Informar os colaboradores sobre os riscos de segurança e as melhores práticas para mitigá-los.

Desenvolver Competências: Ensinar habilidades específicas, como reconhecer ataques de phishing e proteger credenciais de acesso.

Promover a Colaboração: Incentivar uma cultura de segurança onde todos, independentemente de suas funções, colaboram para um ambiente seguro.

Reforçar Políticas Internas: Alinhar todos os colaboradores às políticas de segurança da FortiCloud, garantindo conformidade e boas práticas.

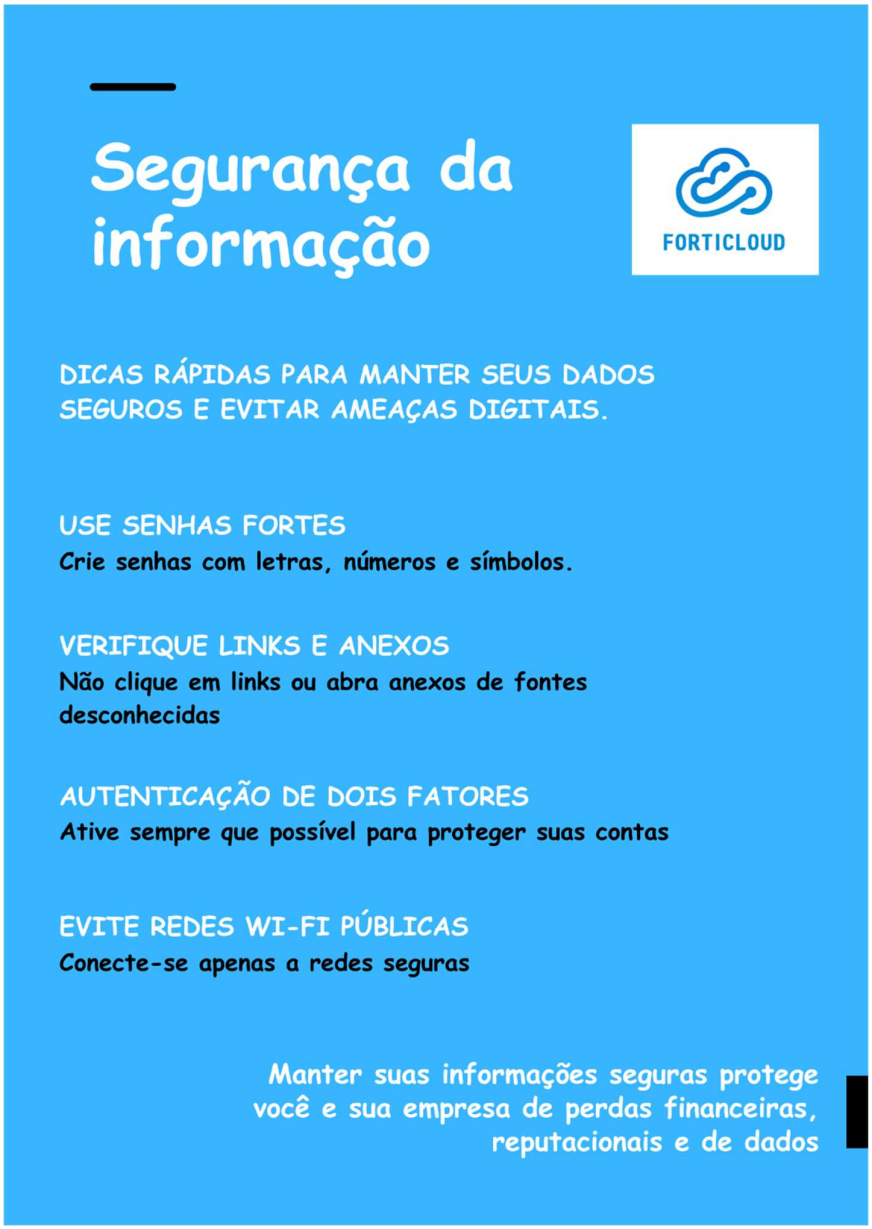
11.3. Envolvimento dos Colaboradores

A participação de todos os colaboradores é fundamental para o sucesso da campanha. A FortiCloud espera que cada membro da equipe esteja engajado nas formações e pratique os conceitos aprendidos no dia a dia. Além disso, haverá atividades interativas, como simulações e competições, que incentivam o envolvimento e a prática ativa. A presença nas formações será acompanhada pela equipe de segurança e recursos humanos, garantindo que todos participem e absorvam os conteúdos essenciais.

11.4. Resultados Esperados

Ao final de uma campanha bem sucedida, espera-se uma equipe mais preparada para enfrentar ameaças cibernéticas e proteger os dados da empresa. A conscientização sobre segurança será incorporada à rotina de trabalho, reduzindo significativamente o risco de incidentes de segurança e fortalecendo a posição da FortiCloud como uma organização segura e confiável.

11.5. Flyer da campanha



12. Outros Conteúdos

O Sistema de Gestão de Segurança da Informação (SGSI) é fundamental para proteger dados e informações estratégicas em um ambiente digital cada vez mais ameaçado por ciberataques e vulnerabilidades. Um SGSI bem implementado ajuda as organizações a mitigar riscos, manter a conformidade com normas como a ISO 27001, e estabelecer uma cultura de segurança que envolve todos os colaboradores. Abaixo, são apresentados insights de especialistas e fontes confiáveis que discutem as vantagens e os impactos do SGSI para a segurança e sucesso das empresas.

12.1. "A Importância do SGSI" por Luciano Ribeiro Navarro

O especialista Luciano Ribeiro Navarro, em seu artigo no LinkedIn intitulado "A Importância do SGSI: Trazendo a cultura de Segurança da Informação nas Empresas", destaca que "no mundo digital altamente conectado em que vivemos, a segurança da informação é um fator crucial para o sucesso e a sobrevivência das empresas." Segundo Navarro, implementar um SGSI é essencial para manter a integridade e a confiança nos processos organizacionais, especialmente em setores com dados sensíveis, como o financeiro e o de saúde.

Para leitura completa: LinkedIn - Luciano Ribeiro Navarro https://www.linkedin.com/pulse/import%C3%A2ncia-do-sgsi-garantindo-seguran%C3%A7a-da-nas-ribeiro-navarro-/

12.2. "Information Security Management System (ISMS) Benefits" por Cyber Management Alliance

A Cyber Management Alliance explica que a implementação de um SGSI baseado na ISO 27001 oferece inúmeras vantagens, incluindo "a proteção da reputação corporativa, a minimização de riscos de incidentes de segurança e a garantia de conformidade regulatória." A empresa também menciona que um SGSI ajuda a estabelecer processos para prevenir, detetar e responder rapidamente a incidentes de segurança, o que é vital para evitar prejuízos financeiros e danos à imagem da organização.

Fonte: Cyber Management Alliance - ISMS Benefits

https://www.cm-alliance.com/information-security-management-system-isms-training-course

12.3. "A Guide to Implementing an Information Security Management System" por Infosec Institute

No artigo do Infosec Institute, a importância do SGSI é associada ao fortalecimento da segurança cibernética e ao aumento da confiança dos clientes e parceiros. Segundo o instituto, "um SGSI bem estruturado ajuda as empresas a estabelecer controles eficientes e a desenvolver uma abordagem proativa contra ameaças." O artigo também aponta que o SGSI melhora a cultura organizacional de segurança, engajando os colaboradores em práticas responsáveis de proteção de dados.

Fonte: Infosec Institute - Guide to ISMS

https://www.infosecinstitute.com/resources/

12.4. Livro: "Information Security Management Principles" por David Alexander et al.

Neste livro, os autores discutem a relevância do SGSI como uma estrutura para identificar, controlar e mitigar riscos à segurança da informação. Eles afirmam que "o SGSI permite uma visão abrangente dos riscos de segurança da informação e fornece uma abordagem sistemática para gerenciá-los." O livro também aborda as boas práticas e as vantagens de uma certificação como a ISO 27001 para melhorar a resiliência organizacional.

Referência: Alexander, D., Finch, A., Sutton, D., & Taylor, A. (2013). Information Security Management Principles. BCS, The Chartered Institute for IT.

13. Considerações Finais

A implementação de um **Sistema de Gestão de Segurança da Informação (SGSI)** na FortiCloud demonstra a importância de um framework estruturado para a proteção de dados em uma empresa altamente exposta a riscos cibernéticos. O desenvolvimento deste projeto evidenciou como um SGSI, alinhado à ISO 27001:2022, contribui para a criação de uma cultura organizacional robusta em segurança da informação, permitindo que a FortiCloud adote uma postura proativa contra ameaças e esteja preparada para responder a incidentes com eficácia.

Ao longo do trabalho, discutimos as principais práticas de segurança da FortiCloud, como políticas de acesso, segurança no teletrabalho, e estratégias de conscientização para colaboradores. A análise SWOT revelou tanto as fortalezas da FortiCloud, como sua infraestrutura global e equipe qualificada, quanto desafios, como os altos custos de manutenção e a complexidade regulatória. O processo de definição das necessidades das partes interessadas, incluindo clientes, reguladores e acionistas, foi essencial para garantir que o SGSI atendesse plenamente às expectativas e exigências de cada grupo.

Os benefícios de um SGSI bem implementado vão além da conformidade regulatória, proporcionando uma vantagem competitiva que fortalece a confiança de clientes e parceiros na FortiCloud. Este projeto reafirma que o investimento em segurança da informação é não só uma medida de proteção, mas também um diferencial estratégico para o crescimento sustentável da empresa. Com a aplicação dos objetivos e políticas definidas, a FortiCloud está preparada para enfrentar as constantes evoluções do cenário digital e garantir a proteção de suas operações e dos dados que lhe são confiados.

Referências Bibliográficas

[1] L. R. Navarro, "A Importância do SGSI: Trazendo a cultura de Segurança da Informação nas Empresas," LinkedIn. [Online]. Disponível em: https://www.linkedin.com/pulse/import%C3%A2ncia-do-sgsi-garantindo-seguran%C3%A7a-da-nas-ribeiro-navarro-/ . Acesso em: 03-nov-2024.

[2] Cyber Management Alliance, "Information Security Management System (ISMS) Benefits," Cyber Management Alliance. [Online]. Disponível em: https://www.cm-alliance.com/information-security-management-system-isms-training-course . Acesso em: 03-nov-2024.

[3] Infosec Institute, "A Guide to Implementing an Information Security Management System," Infosec Institute. [Online]. Disponível em: https://www.infosecinstitute.com/resources/. Acesso em: 03-nov-2024.

[4] D. Alexander, A. Finch, D. Sutton, and A. Taylor, Information Security Management Principles. Swindon, U.K.: BCS, The Chartered Institute for IT, 2013.