1

Organização da Segurança da Informação

Segurança e Auditoria de Sistemas

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Gestão da Segurança da Informação: como implantar na prática

Segurança da informação é a palavra do momento. Todas as organizações, sejam elas de pequeno, médio ou grande porte, sejam elas focadas em TI ou que possuem áreas de TI que suportam o negócio já estão sendo, de forma direta ou indireta, impactadas pela preocupação do mercado (empresas e pessoas) com a segurança da informação. É bastante provável que a sua organização lide com dados sensíveis e/ou informações estratégicas internas, independentemente de seu tamanho.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Gestão da Segurança da Informação: como implantar na prática

Para pequenas e médias empresas (PMEs), implantar uma gestão eficaz de segurança da informação pode ser um desafio, mas é fundamental para proteger seus ativos e garantir a continuidade dos negócios, dado que para esse nicho de organizações, incidentes de segurança podem decretar o fim de suas operações. Neste artigo buscamos esclarecer alguns tópicos essenciais e também fornecer um guia prático (ainda que em alto nível), que pode ajudar PMEs a entender e implementar uma estratégia de segurança da informação.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

O que é a Gestão de Segurança da Informação?

A gestão de segurança da informação envolve um conjunto de políticas, processos e controles técnicos destinados a proteger toda e qualquer informação julgada como relevante para uma organização contra ameaças internas ou externas, garantindo a confidencialidade, integridade e disponibilidade dessas informações. Gestão de Segurança da Informação faz parte do que chamamos comumente de governança corporativa, bastante alinhada às melhores práticas e normas, como a ISO/IEC 27001.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

O que é a Gestão de Segurança da Informação?

No contexto da segurança da informação, a confidencialidade, a integridade e a disponibilidade (muitas vezes abreviadas como CIA) são três princípios fundamentais que constituem a pedra angular das políticas e práticas de segurança da informação. Aqui está o que cada princípio envolve:

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

O que é a Gestão de Segurança da Informação?

Mas o que é confidencialidade, a integridade e a disponibilidade?

- Confidencialidade:

  A confidencialidade garante que as informações sejam acessíveis apenas às pessoas autorizadas a ter acesso. O objetivo, portanto, é impedir a divulgação não autorizada de informações confidenciais, como dados pessoais, propriedade intelectual ou informações governamentais classificadas. Algumas formas de se conseguir confidencialidade de dados é através do uso de criptografia, controles de acesso, mascaramento de dados e canais de comunicação seguros.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

O que é a Gestão de Segurança da Informação?

- Integridade:

  A integridade garante que as informações sejam precisas, consistentes e confiáveis durante todo o seu ciclo de vida. Tem como foco manter a confiabilidade dos dados e sistemas, evitando modificações ou adulterações não autorizadas. Técnicas que podem auxiliar a garantir a integridade incluem checksums, assinaturas digitais, controle de versão e controles de acesso para garantir que apenas indivíduos autorizados possam modificar os dados.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

O que é a Gestão de Segurança da Informação?

- Disponibilidade:

  A disponibilidade garante que as informações e os sistemas sejam acessíveis e utilizáveis quando necessário por usuários autorizados. Enfatiza a importância de prevenir interrupções no acesso e garantir acesso oportuno e confiável a informações e serviços. A disponibilidade pode ser garantida através da implementação de redundância (por exemplo, backups, sistemas de failover), plano de recuperação de desastres, sistemas tolerantes a falhas e design de rede robusto.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

O que é a Gestão de Segurança da Informação?

Esses princípios formam coletivamente a base para projetar e implementar medidas de segurança que protejam dados e sistemas contra acesso não autorizado, alteração e tempo de inatividade. São considerações essenciais nas estratégias de segurança digital e física em vários setores e indústrias.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Passo a Passo para Implantação

1. Compreender a necessidade e obter suporte da Alta Direção

Por que?

Sem o apoio da alta direção, qualquer iniciativa de implantação de governança corporativa, incluindo a de segurança, estará destinada ao fracasso. O comprometimento e patrocínio dos líderes é crucial para a alocação de recursos e o estabelecimento de uma cultura de segurança. Sem eles, dificilmente os novos padrões, políticas e procedimentos serão seguidos por todos.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Passo a Passo para Implantação

1. Compreender a necessidade e obter suporte da Alta Direção

Como?

- Realize apresentações para a alta direção explicando a importância da segurança da informação.
- Use exemplos de incidentes reais que impactaram outras empresas.
- Destaque os benefícios, como a proteção contra violações de dados e conformidade com regulamentações.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Passo a Passo para Implantação

2. Realizar uma avaliação de riscos

Por que?

Identificar e entender os riscos é o primeiro passo para gerenciá-los eficazmente. Nem todas as informações dentro das organizações possuem o mesmo nível de importância. Portanto, uma avaliação de riscos fará com que a organização entenda onde focar seus esforços para proteger aquilo que realmente importa.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Passo a Passo para Implantação

2. Realizar uma avaliação de riscos

Como?

- **Identificação de Ativos**: Liste todos os ativos de informação (documentos, banco de dados, sistemas, etc.).
- **Identificação de Ameaças e Vulnerabilidades**: Identifique possíveis ameaças (hackers, desastres naturais, erro humano) e vulnerabilidades.
- **Avaliação de Impacto**: Avalie o impacto de possíveis incidentes de segurança.
- **Probabilidade de Ocorrência**: Estime a probabilidade de cada ameaça ocorrer.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Passo a Passo para Implantação

3. Desenvolver políticas de segurança

Por que?

Políticas claras são essenciais para definir expectativas e responsabilidades. Elas precisam ser escritas de forma compreensível para qualquer pessoa dentro da organização, seja ela de amplo conhecimento técnico ou não. No caso da SI, essas políticas devem estabelecer regras de como a organização e seus colaboradores devem atuar para garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Passo a Passo para Implantação

3. Desenvolver políticas de segurança

Como?

- **Política de Senhas**: Defina requisitos para a criação e atualização de senhas.

- **Política de Uso Aceitável**: Estabeleça diretrizes para o uso aceitável dos recursos de TI. Trata-se de um conjunto de diretrizes e regras para definir como os recursos de TI (equipamentos, dispositivos e softwares) podem ser utilizados pelos funcionários, contratados e, em alguns casos, pelos usuários externos.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Passo a Passo para Implantação

3. Desenvolver políticas de segurança

Como?

- **Política de Senhas**: Defina requisitos para a criação e atualização de senhas.

- **Política de Uso Aceitável**: Estabeleça diretrizes para o uso aceitável dos recursos de TI. Trata-se de um conjunto de diretrizes e regras para definir como os recursos de TI (equipamentos, dispositivos e softwares) podem ser utilizados pelos funcionários, contratados e, em alguns casos, pelos usuários externos.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Passo a Passo para Implantação

3. Desenvolver políticas de segurança

Como?

- **Política de Backup**: Backups são uma poderosa fonte de recuperação em caso de perda de dados. Determine a frequência e os procedimentos para backup de dados.

- **Política de Controle de Acesso**: Defina quem tem acesso a quais informações e sistemas e como isso é controlado.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Passo a Passo para Implantação

4. Implementar controles de segurança

Por que?

Controles são as medidas práticas que protegem os dados.

Como?

- **Controles Físicos:** Instale câmeras de segurança, sistemas de alarme e controle de acesso físico.
- **Controles Técnicos:** Utilize firewalls, software antivírus e criptografia.
- **Controles Administrativos:** Realize treinamentos regulares de segurança para funcionários e defina procedimentos de resposta a incidentes.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação
Passo a Passo para Implantação
5. Educar e treinar funcionários

Por que?

Os funcionários são a primeira linha de defesa contra ameaças à segurança. É muito comum que as falhas de segurança sejam provenientes de falhas humanas. E muitas vezes essas falhas humanas ocorrem por falta de treinamento e capacitação dos profissionais;

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação

Passo a Passo para Implantação

5. Educar e treinar funcionários

Como?

- **Programas de Treinamento:** Realize treinamentos periódicos sobre políticas de segurança e práticas recomendadas.
- **Simulações de Phishing:** Realize testes de phishing para educar os funcionários sobre ameaças de engenharia social.
- **Campanhas de Conscientização:** Promova a conscientização contínua sobre segurança através de campanhas internas.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação
Passo a Passo para Implantação
6. Monitorar e revisar regularmente

Por que?

A segurança da informação é um processo contínuo que requer monitoramento e melhorias constantes. É necessário ficar atento aos ataques para entender se os controles de segurança da informação implantados foram efetivos e/ou precisam ser aprimorados. Além disso, a monitoração pode detectar tendências futuras de ataques.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação
Passo a Passo para Implantação
6. Monitorar e revisar regularmente

Como?

- **Monitoramento Contínuo:** Utilize ferramentas para monitorar o tráfego de rede e detectar atividades suspeitas.
- **Auditorias e Revisões:** Realize auditorias internas regulares e revise as políticas de segurança periodicamente.
- **Gestão de Incidentes:** Tenha um plano de resposta a incidentes e realize testes de resposta a incidentes.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação
Passo a Passo para Implantação
6. Monitorar e revisar regularmente

Como?

- **Monitoramento Contínuo:** Utilize ferramentas para monitorar o tráfego de rede e detectar atividades suspeitas.
- **Auditorias e Revisões:** Realize auditorias internas regulares e revise as políticas de segurança periodicamente.
- **Gestão de Incidentes:** Tenha um plano de resposta a incidentes e realize testes de resposta a incidentes.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação
Passo a Passo para Implantação
7. Adotar uma abordagem de melhoria contínua

Por que?

As ameaças estão em constante evolução, portanto, sua abordagem à segurança também deve evoluir, de preferência numa frequência mais rápida do que as ameaças.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação
Passo a Passo para Implantação
7. Adotar uma abordagem de melhoria contínua

Como?

- **Feedback Regular:** Colete feedback dos funcionários sobre as políticas e procedimentos de segurança.
- **Atualizações Tecnológicas:** Mantenha os sistemas e software atualizados com os patches de segurança mais recentes.
- **Revisão de Riscos:** Reavalie os riscos periodicamente para identificar novas ameaças e vulnerabilidades.

Segurança e Auditoria de Sistemas

Organização da Segurança da Informação
Passo a Passo para Implantação
Ferramentas e Recursos Úteis

Para ajudar na implementação da gestão de segurança da informação, considere utilizar ferramentas que apoiem as atividades acima descritas. Adote frameworks de segurança reconhecidos, como a ISO/IEC 27001, o CIS Controls e o NIST Cybersecurity Framework, para guiar suas práticas de segurança.

Lembre-se de que a segurança da informação é um processo contínuo e dinâmico. Ameaças novas e emergentes exigem que as políticas e práticas de segurança sejam revisadas e atualizadas regularmente. Com comprometimento, planejamento e execução cuidadosa, sua empresa pode construir um ambiente seguro e resiliente contra ameaças cibernéticas.

Referências

- https:///promovesolucoes.com/gestao-da-seguranca-da-informacao-guia-pratico-para-pmes/