Como Elaborar Plano de Segurança da Informação

Logo abaixo descrevo um passo a passo, como exemplo, de etapas para se fazer um plano de segurança da informação:

1. Selecionar Participantes para o Processo Planejamento

Nessa fase deve ser definido quem irá participar do planejamento da segurança da informação.

Nesse sentido, é preciso escolher os participantes que faram parte do processo de planejamento, entre eles, podemos incluir: o gestor de TI, o gestor de segurança física, também é importante que os gestores de outras áreas da empresa façam parte desse processo. Afinal, são eles que irão transmitir para os colaboradores quais as orientações que deverão ser seguidas.

Outro ponto importante do planejamento é avaliar a vulnerabilidade dos dados da empresa. Para tanto, o gestor do departamento de TI da empresa é a pessoa responsável para realizar essa análise.

Com esses dados em mãos, o profissional conseguirá definir quais as boas práticas da segurança da informação deverão ser aplicadas por cada área.

2. Elaborar Política de Segurança da Informação

Nessa fase, com base nas melhoras práticas e normas de segurança da informação, deve-se definir a Política de Segurança da Informação (PSI) a ser adotada por todo a organização.

3. Realizar Inventário de Ativos

Ativo é tudo aquilo que tem valor para a organização. Assim, pode-se definir ativo como qualquer elemento que sustenta um ou mais processos de trabalho de uma unidade ou de uma área da organização.

Inventariar os ativos associados a informação e classificá-los de acordo com sua relevância para a organização e seus processos de trabalho é ação que deve preceder iniciativas como a classificação da informação e a avaliação de risco em segurança da informação.

Fonte: Blog Gestão de Segurança Privada - Parte do Artigo: Plano de Segurança da Informação (PSI): O que, Como Elaborar, Exemplo. Disponível em: https://gestaodesegurancaprivada.com.br/plano-de-seguranca-da-informacao-psi-o-que-como-elaborar-exemplo/

O inventário de ativos associados a informação e aos recursos de processamento da informação deve registrar aqueles relevantes no ciclo de vida da informação e descrever a sua importância para o funcionamento da instituição.

O inventário deve ainda explicar o ciclo de vida da respectiva informação: a criação, o processamento, o armazenamento, a transmissão, a exclusão e, ao fim do ciclo, se necessário, o seu descarte seguro.

Os ativos devem ser qualificados também por outras informações relevantes, como localização, responsável e modo de recuperação em caso de desastre.

Para cada ativo identificado no inventário, é recomendável que seja definido um responsável encarregado de manter os seus controles de segurança, com o objetivo de diminuir chances de que eles tenham a segurança comprometida.

Um inventário completo deve abranger ativos pertencentes a várias categorias, por exemplo:

a) Processos e atividades do negócio:

- Processos críticos cuja interrupção impossibilita o cumprimento da missão da organização;
- Processos que, se modificados, podem afetar o cumprimento da missão;
- Processos necessários para a conformidade com requisitos legais ou regulatórios; etc.;

b) Ativos de informação:

- Informação vital para o cumprimento da missão;
- Informação de alto custo de obtenção;
- Informação estratégica essencial para a tomada de decisão;
- Informação em papel, em meio digital ou qualquer outro suporte;

c) Ativos de software:

- Sistemas de informação,
- Softwares aplicativos desenvolvidos, licenciados ou adquiridos pela organização;
- Software de prateleira;

Fonte: Blog Gestão de Segurança Privada - Parte do Artigo: Plano de Segurança da Informação (PSI): O que, Como Elaborar, Exemplo. Disponível em: https://gestaodesegurancaprivada.com.br/plano-de-seguranca-da-informacao-psi-o-que-como-elaborar-exemplo/

- Sistemas operacionais;
- Software básico, etc.;

d) Ativos físicos:

- Dispositivos fixos ou móveis de processamento;
- Periféricos;
- Mídia de armazenamento;
- Instalações físicas;
- etc.;

e) Serviços:

- Serviços de computação de terceiros;
- Rede de dados;
- Serviço de transporte de dados (aluguel de link);
- Serviço de fornecimento de energia elétrica, etc.;

f) Pessoas:

- Empregados;
- Prestadores de serviços;
- Parceiros;
- Fornecedores;
- Visitantes;
- Clientes;
- Etc;

g) Organização:

- Estrutura organizacional;
- Infraestrutura organizacional;

h) Ativos Intangíveis:

- Imagem da instituição, reputação, credibilidade, etc.

9.3.1 Resultados esperados:

- Conhecimento abrangente dos ativos de informação da organização, com definição de seus atributos e dos responsáveis por controlar sua segurança;

Fonte: Blog Gestão de Segurança Privada - Parte do Artigo: Plano de Segurança da Informação (PSI): O que, Como Elaborar, Exemplo. Disponível em: https://gestaodesegurancaprivada.com.br/plano-de-seguranca-da-informacao-psi-o-que-como-elaborar-exemplo/

- Possibilidade de classificação dos ativos de informação como ostensivos, de acesso restrito ou sigilosos, com o respectivo grau de sigilo;
- Possibilidade de gestão dos riscos com base nas características dos ativos inventariados.

4. Edição de Norma sobre Classificação de Informações

Editar norma que estabeleça critérios, procedimentos e responsabilidades para a classificação das informações segundo o grau de proteção requerido, além de criar os controles voltados a garantir que o grau de proteção atribuído à informação seja efetivamente observado ao longo de seu ciclo de vida.

Implantar o processo de classificação preconizado pela norma e implantar o acompanhamento dos controles nela estabelecidos.

Importância da classificação da informação

A classificação torna possível a adoção de medidas de proteção proporcionais à importância ou à reserva de acesso que caracteriza uma informação específica.

Entre os vários critérios aplicáveis à classificação da informação, dois são particularmente importantes do ponto de vista da Segurança da Informação:

- **o valor da informação e seu grau de sigilo.**

A classificação da informação quanto ao seu livre acesso, ou à restrição de acesso, ou ainda quanto ao seu grau de sigilo (reservada, secreta ou ultrassecreta), é condição necessária para que, nos casos aplicáveis, se possa preservar sua confidencialidade.

4.1 Resultados esperados

- Proteção das informações classificadas na proporção de seu gra u de sigilo ou de restrição de acesso;
- Uso adequado e proporcional de recursos e controles de proteção de informações;
- Atribuição de responsabilidades a quem deve classificar, quem deve proteger e quais cuidados o usuário deve tomar ao lidar com informações classificadas ou de acesso restrito;

- Provimento de elementos necessários à implantação da gestão de riscos, que depende do inventário de ativos e da classificação das informações.

5. Implantação Sistema de Gerenciamento de Risco de Segurança da Informação

Tem como objetivo gerir os riscos relativos à segurança da informação, visando à redução da incerteza decorrente de ameaças a que a informação está exposta.

O gerenciamento de risco consiste em um conjunto de ações e controles que visam reduzir a possibilidade de materialização de riscos a que uma informação está exposta.

O risco em relação à segurança da informação pode ser definido como o potencial de que uma dada ameaça explore vulnerabilidades da organização visando causar dano, perda, acesso indevido ou indisponibilidade aos ativos de informação.

A implantação da Gerenciamento de Riscos em Segurança da Informação envolve, ao menos, as seguintes atividades:

- Selecionar metodologia de gerenciamento de risco mais indicada;
- Capacitar colaboradores para a gestão de risco de Segurança da Informação;
- Identificar, analisar e avaliar os riscos relativos aos ativos de informação da organização (requer a realização prévia do Inventário de Ativos);
- Tratar os riscos identificados e avaliados, modificando-os, evitando os, compartilhando-os ou assumindo-os e, depois, documentar e comunicar os riscos assumidos às partes interessadas;
- Implantar a gestão de risco como processo organizacional, a ser realizado periodicamente em um ciclo PDCA (Plan – Do – Check – Act) de melhoria contínua.

5.1 Resultados esperados:

- Redução do risco de incidentes que possam resultar em perda, dano, indisponibilidade ou acesso indevido à informação;
- Redução dos custos decorrentes de incidentes;
- Aprimoramento da segurança e disponibilidade dos serviços e sistemas de Tecnologia da Informação;

Fonte: Blog Gestão de Segurança Privada - Parte do Artigo: Plano de Segurança da Informação (PSI): O que, Como Elaborar, Exemplo. Disponível em: https://gestaodesegurancaprivada.com.br/plano-de-seguranca-da-informacao-psi-o-que-como-elaborar-exemplo/

- Impacto positivo na credibilidade da instituição;
- Cumprimento de leis, regulamentos e recomendações do controle.

6. Implantação de Sistema de Gestão da Segurança da Informação (SGSI)

Tem como objetivo dotar a instituição de meios para acompanhar e gerir as iniciativas em Segurança da Informação que permeiam todas as áreas, visando minimizar a ocorrência de incidentes, tais como indisponibilidade, perda, acesso indevido ou alteração indevida da informação, com foco nos controles apropriados aos processos de trabalho da organização.

Um Sistema de Gestão da Segurança da Informação também torna possível a certificação, por organismos independentes, da conformidade da instituição em relação às boas práticas em Segurança da Informação previstas nas normas brasileiras.

7. Campanha de Conscientização em Segurança da Informação

Tem como objetivo assegurar a conscientização dos empregados, prestadores de serviço e fornecedores em relação a responsabilidades e atitudes no sentido de preservar a Segurança da Informação no âmbito da organização.

A ação de sensibilização dos colaboradores ao tema da Segurança da Informação é iniciativa fundamental para torná-los cientes das suas responsabilidades e conhecedores das práticas e métodos aplicáveis à proteção da informação.

É importante que os conceitos e a relevância da Segurança da Informação passem a fazer parte da cultura empresarial da organização.

A campanha deve estar alinhada com as políticas e os procedimentos relevantes para a proteção da disponibilidade, da integridade e, quando for o caso, da confidencialidade dos ativos de informação.

Deve se divulgar a importância da informação para a instituição, o comprometimento da direção com a preservação da Segurança da Informação, as responsabilidades estabelecidas na Política de Segurança da Informação para as unidades administrativas e para os usuários, além dos

Fonte: Blog Gestão de Segurança Privada - Parte do Artigo: Plano de Segurança da Informação (PSI): O que, Como Elaborar, Exemplo. Disponível em: https://gestaodesegurancaprivada.com.br/plano-de-seguranca-da-informacao-psi-o-que-como-elaborar-exemplo/

procedimentos e controles a serem adotados com vistas à proteção da informação.

Uma campanha, para ser efetiva, requer o emprego de diferentes formas de comunicação da informação, como ciclos de palestras, cartazes, folhetos, notas informativas, boletins periódicos e sítio intranet sobre o tema.

Deve levar em conta os diferentes papéis desempenhados pelos colaboradores na instituição.

Deve ainda prever que as ações de conscientização sejam revistas regularmente, de forma a atingir novos colaboradores que passem a integrar os quadros da instituição.

É recomendável que a campanha contemple sensibilização específica para os colaboradores que venham a ocupar novas posições na instituição, preferencialmente antes de assumirem as novas atribuições.

A própria campanha deve ser atualizada regularmente, de modo a permanecer alinhada com as políticas e os procedimentos da instituição e incorporar lições aprendidas a partir de incidentes de Segurança da Informação reais vividos pela instituição.

a) Resultados esperados:

Colaboradores conscientes da importância de se preservar a Segurança da Informação em seus processos de trabalho e treinados em como mantê-la.

Redução da ocorrência de incidentes de Segurança da Informação.

Fonte: Blog Gestão de Segurança Privada - Parte do Artigo: Plano de Segurança da Informação (PSI): O que, Como Elaborar, Exemplo. Disponível em: https://gestaodesegurancaprivada.com.br/plano-de-seguranca-da-informacao-psi-o-que-como-elaborar-exemplo/

Fonte: Blog Gestão de Segurança Privada - Parte do Artigo: Plano de Segurança da Informação (PSI): O que, Como Elaborar, Exemplo. Disponível em: https://gestaodesegurancaprivada.com.br/plano-de-seguranca-da-informacao-psi-o-que-como-elaborar-exemplo/