Política de Segurança da Informação (PSI)

1. **Objetivo**

A Política de Segurança da Informação tem como finalidade atribuir diretrizes e controles para proteger as informações da organização, promovendo a confidencialidade, integridade e disponibilidade dos dados. Tem como objetivo mitigar riscos, garantir conformidade com legislações e normativas, e revigorar a segurança dos ativos de informação.

2. Público-Alvo

Esta política será implementada para todas as áreas da empresa, incluindo desde a área administrativa, setores de desenvolvimento, marketing até o pessoal autorizado que acessa o data center.

3. Conceitos

Pilares da Segurança da Informação:

- Confidencialidade: Assegura que as informações sejam acessíveis apenas por indivíduos com autorização.
- Integridade: Garante a precisão e confiabilidade das informações, impedindo modificações não autorizadas.
- Disponibilidade: Assegura que as informações estejam disponíveis quando no momento em que forem necessárias.

Diretrizes, Controles e procedimento:

- Diretrizes: Orientações específicas para que os objetivos de segurança sejam atingidos .
- Controles: Procedimentos atribuídos para que as diretrizes sejam atendidas.
- Procedimento: Uma união de etapas sequenciais detalhadas que devem ser acompanhadas para efetivar uma atividade específica. No

contexto de segurança, isso pode ser uma gama de medidas específicas para lidar com incidentes, configurar segurança em sistemas, etc.

4. ISO27000

A Política de Segurança da Informação terá como base as diretrizes da família ISO 27000, em especial a ISO 27001 e 27002. A ISO 27000 é um grupo de normas que determina padrões para sistemas de gestão de segurança da informação, concedendo um referencial para práticas seguras.

5. Legislação

A PSI vai estar em conformidade com as legislações vigentes em relação à segurança da informação. Abrangendo a Lei Geral de Proteção de Dados (LGPD), que é uma legislação brasileira que propõe regras para o tratamento de dados pessoais por organizações, sejam elas públicas ou privadas, com o objetivo de assegurar a privacidade, transparência e segurança das informações dos titulares dos dados. A LGPD fornece aos indivíduos maior controle sobre seus dados pessoais e determina obrigações e responsabilidades para as entidades que os processam. E também abrangendo outras regulamentações convenientes. A conformidade com as normativas objetiva salvaguardar os direitos e privacidade das pessoas.

6. Diretrizes

A. Implementação de Autenticação Multifatorial:

1. Atribuir autenticação multifatorial para acesso a sistemas críticos.

- Implementar um sistema que requer a autenticação multifatorial para acessar sistemas críticos, envolvendo o uso de pelo menos dois fatores de autenticação, como senha e token, para reforçar a segurança.

2. Propor treinamentos habituais sobre o uso e relevância da autenticação multifatorial.

- Realizar treinamentos regulares para todos os usuários, destacando a importância da autenticação multifatorial, instruindo sobre seu uso adequado e esclarecendo dúvidas.

3. Monitorar e analisar constantemente os logs de autenticação para verificar atividades suspeitas.

- Implementar ferramentas de monitoramento contínuo para analisar os logs de autenticação, identificando padrões suspeitos ou atividades não autorizadas. Estabelecer procedimentos claros para responder a incidentes.

B. Criptografia de Dados em Repouso:

1. Criptografar dados cadastrais e informações bancárias armazenados no servidor de banco de dados.

- Implementar algoritmos de criptografia robustos para proteger dados cadastrais e informações bancárias armazenados no servidor de banco de dados, garantindo que mesmo em repouso, os dados permaneçam seguros.

2. Atualizar políticas de segurança para abranger a criptografia como requisito.

- Rever e aprimorar as políticas de segurança para explicitamente incluir a criptografia como um requisito mandatório em todas as fases do armazenamento de dados, assegurando conformidade.

3. Propor auditorias regulares para assegurar a efetividade da criptografia atribuída.

- Planejar auditorias frequentes para avaliar a eficácia da criptografia implementada, garantindo que os algoritmos utilizados estejam atualizados e ofereçam um nível adequado de segurança.

C. Acesso Restrito e Monitoramento de Alterações:

1. Restringir o acesso ao servidor de catálogos somente a usuários com autorização.

- Configurar políticas de acesso que permitam apenas a usuários autorizados visualizar e modificar os catálogos. Utilizar autenticação forte e autorizações baseadas em função.

2. Atribuir mecanismos de monitoramento de alterações nos catálogos.

- Implementar ferramentas de monitoramento que registrem e alertem sobre quaisquer alterações nos catálogos, incluindo quem fez a alteração e quando, proporcionando rastreabilidade.

3. coordenar auditorias periódicas nas permissões de acesso.

- Realizar auditorias regulares nas permissões de acesso, garantindo que somente usuários autorizados tenham acesso aos catálogos. Corrigir quaisquer discrepâncias encontradas durante as auditorias.

7. Sanções

A não obediência da PSI pode acarretar em ações disciplinares, contendo advertências, suspensões, e, em casos críticos, rescisão de contrato de trabalho, de acordo com a magnitude do descumprimento.

8. Auditoria

A Auditoria é uma avaliação ordenada e independente dos controles, processos e práticas de segurança implantadas pela organização.

A auditoria de PSI será baseada na revisão regular das práticas de segurança atribuídas. Serão conduzidas auditorias internas e externas, abrangendo análises de conformidade, fiscalização de logs e avaliação do êxito dos controles implementados.

9. Gestão de Incidentes

O plano de incidentes baseia-se na gestão de riscos efetuada, incluindo procedimentos para identificação, registro, resposta, recuperação e lições aprendidas. A equipe de resposta a incidentes será designada e treinada para garantir uma ação rápida e eficaz em caso de violação.

10. Comitê da PSI

O Comitê da PSI é formado por integrantes de diversos setores, abrangendo representantes da administração, TI, segurança da informação e jurídico. O comitê é encarregado de fiscalizar e atualizar regularmente a PSI, assegurando sua eficiência e conformidade constante.

11. Conclusão

A aplicação da PSI irá gerar ganhos significativos à empresa, revigorando a segurança da informação, protegendo os dados dos clientes, assegurando conformidade legal e conservando a reputação da organização diante das partes interessadas.

Este documento é parte constituinte da estratégia da empresa para certificar a segurança da informação e deve ser revisado constantemente para preservar sua eficiência diante das mudanças e atualizações no ambiente de negócios e nas ameaças cibernéticas.

Plano de Comunicação - Implementação de Autenticação Multifatorial:

Objetivo: Internalizar a importância e os procedimentos da autenticação multifatorial para garantir a segurança dos sistemas críticos.

Canais de Comunicação:

E-mail Inicial:

Destacar a necessidade da autenticação multifatorial.
Explicar benefícios e importância para a segurança.
Infográficos e Cartazes:

Ilustrar o processo de autenticação multifatorial.
Reforçar a ideia nos espaços comuns da empresa.
Treinamento Online:

Módulo específico sobre a implementação da autenticação multifatorial.
Demonstração prática de como utilizar.
Feedback Interativo:

Canal específico para esclarecimento de dúvidas sobre a autenticação multifatorial.
Incentivar a participação ativa.

Avaliação de Compreensão:

Quiz Interativo:

Questões específicas sobre a autenticação multifatorial.

Plano de Comunicação - Criptografia de Dados em Repouso:

Objetivo: Garantir o entendimento e a aplicação correta da criptografia de dados em repouso para proteger dados cadastrais e informações bancárias.

Canais de Comunicação:

E-mail Inicial:

Destacar a importância da criptografia de dados em repouso.
Explicar como isso protege informações sensíveis.
Infográficos e Cartazes:

Ilustrar como a criptografia atua na proteção de dados.
Reforçar a mensagem em locais estratégicos.
Treinamento Online:

Módulo dedicado à aplicação da criptografia de dados em repouso.
Orientações práticas para implementação.
Feedback Interativo:

Canal específico para dúvidas sobre a aplicação da criptografia.
Estímulo à participação ativa.
Avaliação de Compreensão:

Quiz Interativo:
Questões específicas sobre a criptografia de dados em repouso.

Plano de Comunicação - Acesso Restrito e Monitoramento de Alterações:

Objetivo: Internalizar práticas de acesso restrito e monitoramento para prevenir alterações não autorizadas nos catálogos de produtos.

Canais de Comunicação:

E-mail Inicial:

Enfatizar a necessidade de acesso restrito aos catálogos.
Explicar como o monitoramento contribui para a segurança.
Infográficos e Cartazes:

Ilustrar como o acesso é restrito e monitorado.
Reforçar a mensagem em áreas visíveis.
Treinamento Online:

Módulo dedicado às práticas de acesso restrito e monitoramento.
Simulações de situações práticas.
Feedback Interativo:

Canal específico para esclarecimento de dúvidas sobre acesso restrito e monitoramento.
Incentivo à participação ativa.
Avaliação de Compreensão:

Quiz Interativo:

Questões específicas sobre as práticas de acesso restrito e monitoramento.

Responsáveis:

Equipe de Segurança da Informação: Desenvolvimento de materiais e treinamentos específicos.

Departamento de Comunicação Interna: Gestão de e-mails, infográficos e cartazes.

Líderes de Departamento: Engajamento e reforço da importância de cada diretriz.

Monitoramento e Melhoria Contínua:

Análises regulares de métricas, avaliação de compreensão e feedback para ajustes contínuos nos planos de comunicação de cada diretriz.

Plano de Auditoria para os Controles Criados:

Objetivo: Assegurar que os controles implementados (autenticação multifatorial, criptografia de dados em repouso, acesso restrito e monitoramento de alterações) estão em conformidade e são eficazes na proteção da segurança da informação.

Etapas da Auditoria:

Revisão Documental:

Verificação dos documentos e políticas relacionados a cada controle.
Certificação de que as diretrizes foram devidamente documentadas e comunicadas.

Avaliação Técnica:

Análise das configurações dos servidores e sistemas relacionados a cada controle.
Verificação da correta implementação da autenticação multifatorial, criptografia, restrição de acesso, e monitoramento.

Testes de Segurança:

Realização de testes de penetração para avaliar a resistência dos sistemas a tentativas de invasão.
Verificação da eficácia da criptografia e autenticação multifatorial.
Monitoramento de Logs:

Análise dos logs de acesso e alterações nos sistemas.
Identificação de padrões ou eventos suspeitos.
Entrevistas e Treinamentos:

Conversas com a equipe de TI para avaliar o entendimento e a aplicação prática das diretrizes.
Verificação de treinamentos e conscientização.

Revisão de Incidentes:
Análise de incidentes de segurança ocorridos desde a implementação das diretrizes.
Identificação de melhorias com base nas lições aprendidas.

Avaliação de Terceiros:
Se aplicável, revisão da conformidade de fornecedores e parceiros com as diretrizes.
Garantia de que terceiros também seguem padrões de segurança.

Relatório de Conformidade:
Elaboração de um relatório detalhado, destacando áreas de conformidade e possíveis melhorias.
Apresentação do relatório para a alta administração.

Frequência da Auditoria:
Realização de auditorias regulares, preferencialmente anuais, para garantir a atualização contínua e a eficácia dos controles implementados.

Plano de Análise Contínua das Diretrizes de Segurança:
Objetivo: Estabelecer um plano de análise contínua para monitorar o cumprimento das diretrizes de segurança e identificar oportunidades de melhoria.

Métricas de Análise:

Taxa de Adoção:
Avaliação do percentual de funcionários que adotaram as práticas de autenticação multifatorial.

Monitoramento de Logs:
Acompanhamento contínuo dos logs para identificar padrões de comportamento suspeito.

Atualização de Políticas:
Verificação regular da atualização de políticas de segurança, garantindo alinhamento com as melhores práticas.

Testes de Simulação:
Realização de simulações periódicas para testar a eficácia dos controles implementados.

Treinamentos e Conscientização:
Acompanhamento da participação e compreensão contínua em treinamentos relacionados às diretrizes.

Feedback dos Funcionários:
Coleta de feedback dos funcionários sobre a aplicação prática das diretrizes.

Indicadores de Incidentes:
Monitoramento de indicadores de incidentes de segurança para identificar tendências ou aumento de atividades suspeitas.

Ações Corretivas:

Treinamentos Adicionais:
Identificação de lacunas de conhecimento e aplicação de treinamentos específicos.

Atualização de Políticas:
Revisão contínua das políticas de segurança para incorporar aprendizados e melhorias.

Ajustes nos Controles:

Implementação de ajustes nos controles de acordo com as recomendações das auditorias.

Comunicação Reforçada:
Reforço da comunicação sobre a importância das diretrizes.

Frequência da Análise:
Análises regulares, preferencialmente trimestrais, para garantir que as diretrizes estejam sendo seguidas e para identificar áreas de aprimoramento contínuo.

Plano Básico de Gestão de Incidentes

Objetivo: Criar um plano de gestão de incidentes para reagir eficientemente a eventos adversos no cenário de segurança da informação, com foco nas vulnerabilidades mapeadas.

1. Incidente: Acesso Não Autorizado ao Data Center

Contramedidas:

Isolamento Rápido:

Identificação imediata do ponto de acesso não autorizado.

Isolamento do servidor afetado para evitar propagação.

Autenticação Biométrica Urgente:

Implementação rápida da autenticação biométrica para reforçar o controle de acesso.

Realização de treinamentos de conscientização sobre a importância da autenticação biométrica.

Análise Forense:

Condução de uma análise forense para entender a extensão do acesso não autorizado.

Coleta de evidências para ações legais, se necessário.

2. Incidente: Vazamento de Dados Bancários

Contramedidas:

Criptografia Emergencial:
Ativação imediata de criptografia para dados bancários em trânsito.
Revisão e reforço das políticas de criptografia.

Monitoramento Intensificado:
Aumento da vigilância nos logs de acesso ao servidor de banco de dados.
Alertas automáticos para atividades suspeitas.

Comunicação Imediata:
Notificação rápida às autoridades regulatórias e clientes sobre o vazamento.
Estabelecimento de um plano de comunicação para mitigar danos à reputação.

3. Incidente: Alteração Não Autorizada de Catálogos

Contramedidas:

Restauração de Backups:
Restauração imediata dos catálogos a partir de backups confiáveis.
Revisão e melhoria dos procedimentos de backup.

Reforço nas Restrições de Acesso:
Implementação imediata de restrições mais rigorosas ao acesso ao servidor de catálogos.
Realização de auditorias adicionais para garantir conformidade.

Análise de Vulnerabilidades:
Condução de uma análise de vulnerabilidades no servidor de catálogos.
Implementação de patches e atualizações de segurança necessárias.

Procedimentos Gerais:

Comitê de Resposta a Incidentes:
Ativação do comitê de resposta a incidentes para coordenar esforços.
Designação de responsabilidades específicas.

Notificação Obrigatória:

Cumprimento das obrigações legais de notificar incidentes relevantes.

Preparação de comunicados de imprensa e mensagens de cliente, se necessário.

Avaliação Pós-Incidente:

Avaliação detalhada de cada incidente.

Atualização contínua dos procedimentos com base nas lições aprendidas.