PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

Projeto apresentado no Eixo 5 do curso superior de Tecnologia em Redes de Computadores como requisito avaliativo.

Orientador: Prof: Luiz Ferreira

Elaborado por:

André Souza

Brandon Hiago

Israel Oliveira Ribeiro

Júlio César Araújo da Luz

SUMÀRIO

INTRODUÇÃO.....03
APRESENTAÇÃO.....04
OBJETIVO.....04
PÚBLICO ALVO 04
DIRETRIZES GERAIS.....05
SEGURANÇA DA INFRAESTRUTURA.....06
CONSCIENTIZAÇÃO E TREINAMENTO.....07
CONSCIENTIZAÇÃO SGSI.....08
REFERÊNCIA.....09

INTRODUÇÃO

A Segurança da Informação (SI) é um conjunto de estratégias de gestão de processos e políticas destinadas a proteger, identificar e combater ameaças que visem ou não as informações digitais de uma determinada empresa ou pessoa. Entre suas responsabilidades, a Segurança da Informação deve estabelecer um conjunto de processos de negócios que protegerão os ativos de informação, independentemente do estado ou formato da informação (em processo ao ser manipulada e gerada, em frente às ameaças a sua confidencialidade, integridade e disponibilidade. Esse conceito constitui a Tríade CIA do inglês correspondente a “Confidentiality, Integrity and Availability" padronizada pela norma ISO/IEC 27001:2013.

Para melhor garantir a segurança das suas informações, uma organização deve implementar um conjunto de políticas e processos conhecidos como Sistema de Gestão da Segurança da Informação (SGSI) ou do termo em inglês “Information Security Management System (ISMS)”, permitindo gerir e coordenar a forma como a segurança da organização e as informações estão disponíveis. Essa abordagem sistêmica permite definir e aplicar medidas que garantam a confidencialidade, integridade e disponibilidade das informações. AISO/IEC 27001:2013 é a norma internacional de gestão de segurança da informação, ela específica de forma padronizada os requisitos para implementação desta abordagem, definindo como operar, monitorar, analisar e melhorar um SGSI de acordo com as necessidades individuais da organização.
trânsito quando está sendo transmitida numa rede ou armazenada em repouso no caso de estar salva num banco de dados, por exemplo).

A SI é definida por Sêmola como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade."(SÊMOLA, 2003). Atualmente a definição conceitual de SI está padronizado pela norma ISO/IEC 17799:2005 (rebatizada e atualizada por ISO/IEC 27002:2013), que em sua introdução define segurança da informação como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.” (ISO/IEC 17799:2005). Portanto podemos definir a SI como o know-how necessário para preservação e proteção da informação

Desta forma o grupo 3, através da seus membros, formaliza o seu comprometimento em garantir a segurança das informações geradas e custodiadas pelos seus integrantes, preservando a sua confidencialidade, integridade e disponibilidade.
Através do seu SGSI (Sistema de Gestão de Segurança da Informação) o grupo estabelece, em seus processos organizacionais, rigoroso controle para proteger as informações contra diversas ameaças, tais como, vazamento, modificação, destruição, acesso não autorizado, indisponibilidade, entre outras.
Este sistema tem como diretriz principal a Política de Segurança da Informação (PSI), e para que as organizações consigam alcançar o resultado de proteger seus ativos essas regras devem ser cumpridas por todos.

APRESENTAÇÃO

A Política de segurança da informação – SGSI é o documento que orienta e estabelece as diretrizes para a proteção dos ativos, orientação quanto a serviços prestados e a prevenção de responsabilidade legal para todos os usuários de TI. Deve-se, portanto, ser cumprida e aplicada em todas as áreas da organização, empresa etc.

Nosso trabalho está baseado nas leis vigentes em nosso país, bem como nas recomendações propostas pelas normas ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação e deverá ser seguida por todos os colaboradores, bem como pelos prestadores de serviço e se aplicam em qualquer meio ou suporte.

É importante ressaltar que este trabalho, está em seu início de desenvolvimento e visa apoiar inicialmente a Lei Geral de Proteção dos Dados, lei: 13.709. Contudo é recomendada Política específica, da Instituição de educação PUC MG. Toda a informação produzida ou recebida pelos usuários como resultado da atividade profissional contratada, pertencerá a instituição portadora futura.

OBJETIVO

O objetivo deste trabalho é estabelecer os princípios que regulamentam a segurança da informação do Grupo 03, visando garantir a confidencialidade, integridade e disponibilidade das informações geradas e custodiadas.
Determinar o comportamento aceitável dos usuários em relação aos recursos disponibilizados e ao uso das informações geradas e/ou custodiadas;

Acesso lógico aos sistemas e serviços; Armazenamento de informações lógicas e físicas; Uso da Internet; Uso do correio eletrônico coorporativo; Uso de dispositivos móveis; Definir os critérios para classificação das informações

PÚBLICO ALVO

Este trabalho é um documento que norteia toda estrutura de TI e se aplica a todos os usuários, prestadores de serviço, clientes e fornecedores que venham a ter acesso e/ou utilizam as informações, os recursos de TIC e/ou demais ativos tangíveis ou intangíveis do Grupo 03.

DIRETRIZES GERAIS

O documento das diretrizes das melhores práticas e normas de segurança da informação relacionadas a conduta, acesso físico, acesso lógico, uso da internet, uso do correio eletrônico, armazenamento de informação, uso de dispositivos móveis e classificação da informação.

As informações e recursos que poderão ser disponibilizados serão considerados patrimônio e devem ser protegidos, considerando os requisitos do negócio e os riscos envolvidos.
O acesso às informações, independente do meio em que estejam armazenadas, devem ser disponibilizadas apenas aos usuários autorizados.

As credenciais de acesso devem ser de uso exclusivo dos colaboradores da empresa, sendo proibido o compartilhamento.
As senhas devem ter pelo menos 8 caracteres, deve conter uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Uma senha antiga só poderá ser usada novamente após duas novas serem utilizadas. A senha expirará após 90 dias. Não poderá utilizar informações pessoais, como nomes, datas de nascimento etc. Fica também obrigatório a utilização de Autenticação em Múltiplos Fatores (MFA) através de SMS, chamada ou aplicativos como Microsoft Authenticator ou Google Authenticator.
O acesso a rede só é permitido por colaboradores autorizados, tendo o controle de acesso definido por grupos de usuários do AD, restringindo acesso a arquivos e navegação.

Inicialmente poderemos definir a Proteção de dados, como um pilar para todas as redes, tanto de grande, médio ou pequeno porte. Inclusive nos últimos anos ganhou maior destaque na política brasileira com implementação da LGPD.
Alguns tópicos a serem mencionados são as políticas de criptografias e confidencialidades dos dados e diretrizes de segurança para armazenamento de dados sensíveis, não sendo por menos que os pilares da LGPD vigente aqui no brasil trata justamente alguns desses assuntos, podendo citar o 4° princípio que diz "A inviolabilidade da intimidade da honra e da imagem", nada mais que uma singela definição que dados sensíveis pertencentes à pessoas naturais vivas devem por lei serem protegidos, trazendo essa breve citação para o trabalho a ser desenvolvidos podemos estipular alguns fundamentos;
Para tratativas de dados em repouso, serão adotados a utilização de um Active Directory para todos os usuários, ativação do BitLocker em todos os discos rígidos. No que diz respeito aos dados em trânsito serão adotados os protocolos L2tp e OpenVpn, caso necessário utilização de vpn's, no compartilhamento de pastas será realizado uma setorização na qual cada setor terá acesso apenas a sua pasta que lhe diz respeito, outra diretriz será a utilização de proxy.
Por questão de resiliência da rede será adotado o armazenamento físico do banco de dados e um backup em nuvem.

SEGURANÇA DA INFRAESTRUTURA

Todos os usuários deverão conhecer e cumprir as orientações definidas na política de segurança da informação.
Os usuários devem zelar pelas informações a que tenham acesso, independente do meio em que estejam armazenados.
Todos os usuários devem registrar incidentes de segurança da informação.
Os usuários devem recomendar mecanismos de proteção para a área de segurança da informação, sempre que identificar a necessidade de melhorar o nível de segurança da informação na organização.

A identificação é fornecida e controlada pela área de pessoal, ou seja, o DP ou RH. Os visitantes devem ser instruídos em relação às regras de acesso às dependências da empresa no momento da sua identificação.
Os colaboradores que encerrarem suas atividades, devem devolver suas identificações no momento do encerramento das atividades.
O acesso, permanência e a circulação nas áreas internas, serão permitido somente às pessoas autorizadas e com uso de identificação em local visível.
O acesso de visitante deve ser registrado e com acompanhamento.

A entrada e saída dos equipamentos de propriedade da empresa deverá ser autorizada e registrada.
A entrada e saída de equipamentos de visitantes é permitida nos locais autorizados pelo visitado.
A conexão dos equipamentos dos visitantes na rede da empresa deverá seguir os critérios definidos pelo setor de SGSI e Infraestrutura. Os equipamentos que armazenam informações confidenciais devem ser posicionados de forma a não permitir acessos indevidos às informações. Todo equipamento ao sair para manutenção externa deverá ter suas informações e configurações descartadas.

A fim de agilizar o controle e segurança, somente equipamentos autorizados pela Gestão de Infraestrutura, podem ter acesso aos sistemas e serviços.
As diretrizes definidas, demonstram uma melhor forma de controle e acesso à infraestrutura da empresa,

O acesso, geração, utilização, classificação, modificação, distribuição, transferência, armazenamento e eliminação das informações, devem ser feitas de acordo com as necessidades da empresa, sendo que estes processos devem estar devidamente documentados. A empresa reserva-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais.
Equipamentos de colaboradores e visitantes autorizados a utilizar os recursos de rede para uso pessoal podem ter acesso somente à rede de visitantes.
O acesso remoto aos sistemas e serviços é permitido somente com autorização da segurança da informação. O compartilhamento sem credenciais (usuário e senha) de acesso aos sistemas e serviços deverá ser revisto, de acordo com as necessidades.

Sistemas e aplicativos desenvolvidos dentro da organização devem ser documentados e controlados quanto às alterações ou correções feitas, com trilhas do que foi feito a guarda segura da biblioteca de fontes. Toda informação necessária para eventual reconstrução dos aplicativos deve constar de sua documentação. Sistemas e aplicativos desenvolvidos fora da organização, de propriedade de terceiros (com licença de uso para a organização), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes etc.) sob custódia de uma entidade idônea, de comum acordo entre a organização e a empresa fornecedora do software. Tais fontes devem sempre ser atualizadas e verificadas quanto à sua validade e sincronização com a versão em uso no ambiente de produção.
O mau uso dos sistemas, feito de forma acidental ou deliberada, deve ser combatido pela segregação das funções de administração do sistema das funções de execução de certas atividades, ou entre áreas de responsabilidade. Tal segregação de funções visa criar controles para evitar fraudes ou conluios no desempenho de atividades críticas do sistema.

CONSCIENTIZAÇÃO E TREINAMENTO

Na era digital em que vivemos, a segurança da informação se tornou uma questão de suma importância. Com o aumento constante das ameaças cibernéticas, organizações e indivíduos estão cada vez mais expostos a riscos que podem comprometer seus dados confidenciais, financeiros e pessoais. Nesse contexto, o desenvolvimento de políticas de conscientização e treinamento dos usuários sobre boas práticas de segurança da informação emerge como um componente crucial para a proteção contra ameaças cibernéticas, como phishing, uso indevido de senhas e ataques de malware.

A conscientização em segurança da informação visa capacitar os usuários a identificar e mitigar potenciais riscos online. Um dos principais desafios é a educação dos usuários sobre a ameaça constante que o phishing representa. Políticas eficazes de conscientização devem fornecer informações claras sobre como identificar e evitar e-mails e mensagens fraudulentas, bem como os passos a serem seguidos caso ocorra uma suspeita de tentativa de phishing. Além disso, a educação sobre o uso seguro de senhas é fundamental. Instruções sobre a criação de senhas robustas, a importância de não compartilhá-las e o uso de autenticação de dois fatores contribuem significativamente para a proteção das contas online.

Ameaças de malware e ransomware também requerem atenção especial. Políticas de treinamento devem educar os usuários sobre a importância de evitar o download de arquivos e aplicativos suspeitos, bem como sobre os riscos de clicar em links desconhecidos. A implementação de softwares antivírus e a realização regular de verificações de segurança são medidas preventivas cruciais que os usuários devem conhecer.
Ao desenvolver políticas de conscientização e treinamento em segurança da informação, algumas práticas recomendadas incluem:

Personalização: As políticas devem ser adaptadas às necessidades específicas da organização e do público-alvo. Conteúdo genérico pode não ser tão eficaz quanto material que ressoa com a realidade dos usuários.

Comunicação Contínua: A conscientização não é um evento único. Ela deve ser uma jornada contínua, com mensagens regulares e atualizadas sobre os últimos tipos de ameaças e táticas utilizadas pelos cibercriminosos.

Abordagem Multicanal: Utilizar diversos canais de comunicação, como e-mails, vídeos, workshops e pôsteres, para alcançar os usuários em diferentes contextos e situações.

Simulações de Phishing: A realização de simulações de phishing pode ser uma maneira eficaz de testar a eficácia da conscientização dos usuários e identificar áreas que necessitam de melhoria.

Incentivos e Reconhecimento: Reconhecer e recompensar os usuários que demonstram um bom entendimento e práticas sólidas de segurança pode motivar a adesão contínua às políticas.
Em resumo, a conscientização em segurança da informação é um pilar fundamental para a proteção das informações sensíveis no ambiente digital atual. Ao desenvolver e implementar políticas de treinamento e conscientização abrangentes, as organizações podem capacitar os usuários a identificar ameaças e adotar medidas proativas para proteger seus dados e recursos. Esse investimento não apenas fortalece a postura de segurança da organização, mas também contribui para a construção de um ambiente online mais seguro para todos.

RESPONSABILIDADE DA SGSI

Gerenciar as atividades de gestão de segurança da informação. Recomendar ações de segurança da informação e apoiar o comitê gestor de segurança da informação em assuntos relacionados à segurança da informação na organização;

Garantir que a informação documentada do SGSI esteja pertinente, atualizada e divulgada conforme apropriado e deverá ser acompanhado o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas. Por isso, tanto a política de TI quanto as normas, deverão ser revisadas e atualizadas sempre que algum fato e/ou evento relevante acontecer. É necessário definir o cronograma de atualização da política de segurança, garantindo que as normas estejam de acordo com as leis gerais que regem um SGSI. As atualizações poderão ser definidas com o time de segurança e gerenciamento da TI.

REFERENCIAS

Norma ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos;

ISO/IEC 27000, Information technology - Security techniques - Information security management.

ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação – Técnicas de Segurança – Código de práticas para controles de segurança da informação.

ABNT NBR ISO/IEC 27005:2011 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação;