TEMA 02
Políticas de Segurança

Habilidades:

- Identificar a importância de processos e métodos para a segurança digital.
- Elaborar e Planejar Políticas de Segurança.
- Entender as siglas e ferramentas usadas nas Políticas de Segurança.

Políticas de Segurança

As políticas de segurança desempenham um papel fundamental na proteção da segurança da informação de uma organização. Elas estabelecem diretrizes, regras e procedimentos que orientam as práticas e comportamentos relacionados à segurança, enquanto fornecem um quadro de referência à implementação e gestão das medidas de segurança.

Até aqui você já conseguiu perceber que, nos dias de hoje, os recursos tecnológicos são vitais para qualquer negócio, assim como a informação é o bem mais precioso de qualquer empresa.

A importância que o mercado vem dando à segurança da informação de modo geral está cada vez mais intrínseca e consolidada, visto que os riscos aumentam a cada dia, assim como as exigências das legislações vigentes. Cabe à empresa se organizar e investir em boas práticas para corrigir as falhas e dar a devida proteção para seus ativos.

Segundo o dicionário, **política** é "*a arte ou ciência de governar*", *ou "arte ou ciência da organização, direção e administração de nações ou estados*". – Oxford Languages.

Você já deve ter conhecido alguém que diz que "**odeia política**", ou até mesmo você pode ser esse alguém. Este termo é muitas vezes tratado com pessimismo, em especial, quando o assunto discutido é associado à corrupção de servidores públicos e outros governantes.

Mas tudo o que fazemos em nossas vidas é baseado em políticas. É através delas que nossa sociedade é regrada e legislada, assim como aperfeiçoamos as tomadas de decisão extremamente delicadas que surgem durante os laços sociais que são pautados e permeados.

Em uma organização também existem políticas, que servem para nortear e organizar as regras que devem ser seguidas pelos colaboradores e categorizar todos os processos de modo geral.

As **políticas de segurança da informação** (**PSI**) vão tratar da padronização das instruções, regras e procedimentos para organizar e aumentar a proteção dos dados contra possíveis vulnerabilidades, ameaças e riscos que possam prejudicar a empresa. Estas diretrizes devem ser seguidas à risca pelos colaboradores do ambiente que reside a organização, seja física, virtual ou ambas.

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO - POLÍTICAS - ESTRATÉGICO
POLÍTICAS COMPLEMENTARES (NORMAS) - NORMAS E PADRÕES - TÁTICO
PROCEDIMENTOS OPERACIONAIS PADRÃO - PROCEDIMENTOS E ORIENTAÇÕES - OPERACIONAL

Uma boa política de segurança é aquela desenvolvida de acordo com o estudo do ambiente em que ela vai ser implementada. **Nenhuma organização é igual a outra**. Sendo assim, algumas normas que

são importantíssimas para uma empresa podem não funcionar ou não serem necessárias para outra, que atua de forma diferente.

O **profissional de Segurança da Informação** deve estar sempre muito atento às mudanças e desenvolvimento da empresa, assim como deve estar antenado com a legislação e, principalmente, se a política a ser implantada está devidamente baseada nos pilares da segurança da informação citados anteriormente. As políticas de segurança implementadas devem sempre ser analisadas em tempos predeterminados a fim de definir possíveis mudanças.

Mecanismos de Segurança

Antes de qualquer coisa, o profissional de S.I. deve estar munido do conhecimento dos mecanismos de segurança, que **são as ferramentas, soluções e ações com o objetivo de implementar a política de segurança, realizar qualquer tarefa relacionada à Segurança da Informação e Cyber Security de maneira correta e garantir que os 5 pilares da S.I. sejam preservados**.

Confidencialidade - Disponibilidade - Integridade - Autenticidade - Irretratabilidade

Podemos definir os mecanismos de segurança em **4 partes fundamentais**:

1 Prevenção – É um conjunto de práticas adotadas para impedir que os ataques cibernéticos realmente aconteçam. Por meio dela, o profissional de S.I. irá elaborar barreiras para impedir que pessoas não autorizadas acessem um local físico ou em algum sistema operacional, o que limita o ambiente ao máximo. Podemos dividir a prevenção em **alguns pilares principais**.

- **Identificação** – Pilar responsável por solicitar o login para o usuário em um sistema ou rede. Através dele que o ambiente identifica quem está acessando naquele momento, justamente para evitar que seja um atacante ou outra pessoa indesejada.
- **Autenticação** – Assim que o usuário é devidamente identificado pelo login, o ambiente de controle solicita uma senha de acesso. Caso esta senha seja a mesma que foi armazenada anteriormente no banco de dados, o usuário é autenticado e seu acesso, permitido.
- **Controle de Acessos** – Responsável por barrar quaisquer acessos que não sejam autorizados. É neste pilar onde se concentra a proteção dos dados e informações já que só manuseia o ambiente caso este permita. Um exemplo de controle de acessos é o próprio Firewall, que ainda veremos neste conteúdo.

2 Mitigação – É a base que tem como objetivo diminuir os impactos dos ataques a um ambiente informático de uma organização. Estes impactos possuem relação com as vulnerabilidades, riscos e ameaças que vimos no tema anterior são um conjunto de práticas e ações contínuas responsáveis por catalogar e notificar os problemas que já existem no ambiente organizacional.

3 Auditoria – Procedimento base realizado para classificar as atividades onde envolveram algum tipo de ameaça ou uso suspeito para o sistema ou rede, cataloga os eventos, facilita o processo de desenvolvimento ou alteração nas políticas de segurança. Nesta etapa, são realizados testes como os ***pentests***, que veremos posteriormente, os quais irão simular ataques cibernéticos realizados por hackers com o objetivo de identificar possíveis falhas ou brechas, e também os scanners de vulnerabilidades, encarregados por realizar uma varredura no ambiente auditado a fim, também, de buscar alguma ameaça.

4 Recuperação – Este é um dos mais importantes mecanismos de segurança e, por muitas vezes,

esquecidos pelos responsáveis. Por mais que exista inúmeras ferramentas importantes para aprimorar a segurança da informação, nenhuma é 100% confiável e vai garantir que o sistema ou rede seja atacado. É necessário estar preparado para uma possível perda de arquivos contendo dados e informações. Por isso que existe a recuperação, capaz de retomar os serviços da organização de maneira ágil através de **técnicas de recuperação de dados e informações**.

Os meios de recuperação mais comuns são:

Disaster Recovery – Recuperação em Desastres é um conjunto de rápidas medidas que devem ser tomadas e foram previamente preparadas com o objetivo de restabelecer o funcionamento do ambiente ou serviço o mais rápido e com o mínimo de investimento e prejuízo possível.

Backup – Procedimento de **cópia de arquivos importantes para o funcionamento do ambiente, assim como dados e informações críticos**. As cópias podem ser armazenadas tanto em dispositivos físicos, como em HDs externos, como também na nuvem (Armazenamento Cloud). Tem como foco preservar estes conteúdos caso aconteça algo com o ambiente que o afete. A rotina de backup pode ser definida através da própria política de segurança, na qual os responsáveis irão avaliar o tempo necessário entre backups. Isso varia para cada organização.

Planejamento e levantamento de requisitos

Para se implementar uma política de segurança da informação, é necessário a princípio um bom planejamento, juntamente com os mecanismos de segurança. Conforme dito acima, uma empresa é diferente da outra e sempre sofre mudanças.

A equipe de S.I. deve levantar todas as necessidades, problemas, práticas de **cada setor** e as falhas dos colaboradores do local, de modo a preparar **uma PSI entendível e aplicável**, além de monitorá-la e alterá-la sempre que necessário.

Para **levantar os requisitos, precisaremos identificar os ativos de dados e informação de toda a empresa**, assim como analisar as tarefas e procedimentos que já são tomados para ter um real diagnóstico das vulnerabilidades existentes e definir quais mudanças podemos fazer para aperfeiçoar a segurança de cada setor.

Alguns exemplos de levantamentos são:

- Verificar se a empresa realiza backups e caso sim, em qual intervalo de tempo e onde este backup é armazenado;
- Checar a vigilância, monitoramento e controle de acesso em diferentes setores e áreas críticas que envolvem riscos (ex: **Sala de servidor, área contendo disjuntores de energia**, etc);
- Analisar os softwares e antivírus instalados nos computadores e servidores, além de checar se são originais e se há atualizações disponíveis;
- Como funciona o gerenciamento de logins, senhas e demais credenciais de controle de acesso.

Percebeu como estes levantamentos impactam todos os setores da organização? Por intermédio deles, podemos desenvolver as políticas de segurança para que todos sejam engajados a praticá-las.

Classificação de ativos de informação

Esta etapa aplicará a organização dos dados e informações da empresa por diferentes grupos, nos

quais os hierarquiza de acordo com o nível de cada colaborador. Lembre-se que podemos ter mais ou menos grupos, conforme cada organização.

Podemos definir os grupos essenciais como:

Públicos: Acessíveis a todos.
Internos: Acessíveis apenas ao setor responsável.
Secretos: Acessível apenas a um agrupamento seleto bem definido. Inacessíveis aos demais.
Confidenciais: Acessíveis apenas a um menor agrupamento também seleto e bem definido. Inacessíveis aos demais.

Tendo esses grupos bem estabelecidos e organizados, será possível criar ou aperfeiçoar os níveis de acesso e reforçar a segurança em grupos críticos. Estes níveis de acesso são pautados na maneira em que o funcionário se desloca a cada área da empresa e, também, em que ele usa a rede.

Desenvolvimento de Regras

Com todo o planejamento elaborado e os dados devidamente classificados e organizados, **chegamos na etapa da criação de normas**. Esta irá abranger todo o comportamento dos funcionários perante os **recursos digitais** e **não digitais** da empresa. As normas poderão, inclusive, serem classificadas de acordo com o setor e nível hierárquico do local. Alguns exemplos de regras que podem ser implementadas:

- Negar acesso em setores críticos;
- Impedir o uso de celulares em setores específicos ou toda a empresa;
- Bloquear sites inadequados;
- Avaliação periódica dos computadores dos funcionários;
- Limitar o uso de programas para cada funcionário e setor.

Alinhamento final

Finalizada todas as etapas anteriores, chegou a hora de apresentar seu trabalho! É **neste momento em que todo o processo será novamente revisado e aprovado pela diretoria e pelo RH**.
Todo o planejamento deve estar muito bem documentado para os setores críticos analisarem sua implementação juntamente com as políticas já existentes, como as políticas de funcionários e leis trabalhistas vigentes.

Implementação e treinamento

Com tudo aprovado, será implantada a mais nova Política de Segurança. Esta é uma das mais delicadas etapas, já que a conscientização e comunicação são essenciais para o sucesso.
A política deve ser documentada e divulgada aos setores e devidamente comunicada a todos os colaboradores, explicada de maneira concisa. A abordagem deve apresentar o que está envolvido e as normas e consequências do descumprimento das mesmas, assim como existem nas demais políticas e leis.
É nessa etapa inclusive que a empresa deve se preparar para treinar seus colaboradores à nova política, assim como preparar tutoriais aos novos que virão. Isso facilitará a propagação e conscientizará o time a seguir todas as normas de segurança, e garantir que todos estejam alinhados.
É interessante a diretoria solicitar aos seus funcionários uma assinatura em forma de termo, se

comprometendo a cumprir as novas políticas de segurança e dando ciência das consequências de não as seguir.
Durante a implementação e periodicamente após dela, deve-se **avaliar os times para sanar eventuais dificuldades e analisar pontos a serem melhorados**. Este alinhamento e correção inicial são fundamentais para que estas ocasiões se tornem rotinas futuramente, encontrando vulnerabilidades.

Controle e Monitoramento

Por fim, compreendemos que a Política de Segurança da Informação é uma das que mais devemos nos atentar. Como está paralelamente ligada à tecnologia e ao meio digital, os profissionais devem se atualizar periodicamente. Novas ameaças surgem todos os dias, assim como novas atualizações e processos.
Nenhuma política é imutável, ou seja, o setor de T.I. deverá atualizar a empresa na mesma proporção que novas tecnologias e ameaças são apresentadas. Desde mudar de antivírus ou até mesmo alterar a periodicidade dos backups, por exemplo. Todas as atualizações vêm para somar e garantir ainda mais a segurança dos ativos de informação.

RESUMO:
As políticas de Segurança da Informação são um conjunto de regras e normas responsáveis por padronizar e diminuir as chances de ataques cibernéticos e acidentes e envolvem os ativos de informação da organização.
Existem as etapas de Planejamento e Levantamento, Classificação, Desenvolvimento, Alinhamento, Implementação e Treinamento e Controle e Monitoramento dos procedimentos, responsáveis por guiar o profissional de S.I. a traçar um plano de política exclusivo e personalizado para cada ambiente organizacional.

ATIVIDADES:

1. O que são políticas de Segurança da Informação e qual é a sua importância em uma organização?

As políticas de Segurança da Informação são um conjunto de regras e normas responsáveis por padronizar e diminuir as chances de ataques cibernéticos e acidentes, envolvendo os ativos de informação da organização. Sua importância reside na proteção dos dados e informações, assegurando a integridade, confidencialidade e disponibilidade desses ativos, fundamentais para o funcionamento seguro e eficiente da organização.

2. Cite três elementos essenciais que devem estar presentes em uma política de Segurança da Informação.

- Planejamento e Levantamento: etapa inicial onde se traça um plano exclusivo e personalizado para o ambiente organizacional.
- Classificação: envolve a categorização dos ativos de informação de acordo com sua importância e sensibilidade.
- Controle e Monitoramento: responsável por guiar o acompanhamento contínuo e ajustes necessários nos procedimentos.

3. Qual é a relação entre as políticas de Segurança da Informação e a proteção dos dados e informações de uma organização?

As políticas de Segurança da Informação estabelecem diretrizes que protegem os dados e informações da organização contra acessos não autorizados, alterações indevidas e perda de dados. Elas ajudam a garantir que os ativos de informação estejam seguros e que a integridade, confidencialidade e disponibilidade dessas informações sejam mantidas.

4. Por que a conscientização e o treinamento dos funcionários são importantes no contexto das políticas de Segurança da Informação?

A conscientização e o treinamento dos funcionários são importantes porque garantem que todos na organização estejam cientes das políticas de Segurança da Informação e saibam como aplicá-las corretamente. Isso ajuda a prevenir erros humanos que poderiam comprometer a segurança dos dados e fortalece a postura de segurança geral da organização.

5. Explique como as políticas de Segurança da Informação contribuem para a conformidade legal e regulatória de uma organização.

As políticas de Segurança da Informação ajudam a garantir que a organização esteja em conformidade com leis e regulamentos relevantes, como as leis de proteção de dados e privacidade. Ao implementar e monitorar essas políticas, a organização pode demonstrar que está tomando as medidas necessárias para proteger informações sensíveis, evitando penalidades legais e danos à reputação.