CHECKPOINT 2 - SECURITY MANAGEMENT
1TDCG - RM97738 - LUANA BANNWART DE ANDRADE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Introdução:

Para garantirmos a proteção das informações da empresa, é criado este documento com o propósito de informarmos a todos os funcionários e terceiros que possuem acesso aos recursos e informações internas da empresa sobre a Política de Segurança da Informação (PSI) da empresa Fictitious Company.

2. Responsabilidades:

Todos os colaboradores da Fictitious Company são responsáveis pelo entendimento e concordância sobre as seguintes normas, procedimentos e políticas da Fictitious Company.

3. Classificação da Informação:

Para um melhor gerenciamento, toda informação recebida ou gerada pela Fictitious Company deve ser classificada e tratada das seguintes formas:

3.1. Informação confidencial:

Informações e dados que requerem o maior nível de sigilo, como informações pessoais dos clientes, dados financeiros, informações estratégicas e segredos comerciais, podendo apenas serem acessadas e conscientizadas por pessoas autorizadas dentro da Fictitious Company.

3.2. Informação restrita:

Informações e dados que requerem um nível intermediário de proteção, mas ainda tratadas com cautela e segurança, como dados de recursos humanos, informações técnicas e dados de produção, podendo ser acessadas também apenas por pessoas autorizadas.

3.3. Informação pública:

Informações que podem ser divulgadas abertamente, podendo ser acessadas por qualquer indivíduo sem causar prejuízos à empresa ou aos seus clientes.

4. Controles de Acesso:

A Fictitious Company é responsável pela implementação de diferentes métodos que contribuam para a proteção de seus dados, tais quais seriam instalados sobre os controles de acesso físico e lógico de seus dispositivos de TI, como equipamentos de informática, sistemas e bancos de dados.

4.1. Controle de acesso físico:

O controle de acesso físico se aplica à segurança física dos equipamentos da empresa e seus armazenamentos, evitando danos significativos à mesma. Inclui prevenções do tipo:

- Uso de fechaduras;
- Salas de servidores protegidas;
- Restringimento do acesso de pessoas não autorizadas às áreas protegidas;
- Monitoramento severo por câmeras.

4.2. Controle de acesso lógico:

O controle de acesso lógico é aplicado diretamente à proteção dos recursos e dados armazenados virtualmente dentro do sistema de informações da empresa, redes ou aplicativos, visando evitar acessos não autorizados nos mesmos. Sua execução é possível a partir dos seguintes métodos:

- Autenticação multifator: verifica a identidade do usuário antes de permitir seu acesso. Pode ser realizado com o uso de senhas, tokens ou autenticação biométrica.
- Criptografia: garante a segurança de arquivos por meio de técnicas de criptografia que só possam ser lidas por usuários autorizados. Os mesmos terão de receber chaves de descriptografia.
- Firewalls: visam proteger a rede corporativa, filtrando o tráfego de entrada e saída da mesma, permitindo ou bloqueando o acesso a determinados recursos dependendo de cada usuário.
- Controle de acesso baseado em atributos: estabelece as permissões de acesso segundo as características do usuário, tais como: seu cargo, sua localização, o tipo de seu dispositivo e seu histórico de acesso (contendo também o horário).
- Monitoramento de segurança: monitora as atividades dos usuários junto dos registros, visando prevenir possíveis ataques ou violações de segurança e agir rapidamente contra elas.

5. Segurança da Rede e proteção contra Malwares:

A Fictitious Company deve garantir a proteção da rede corporativa em função de privar os dados que transitam nela e implementar também, em todos seus dispositivos e sistemas, prevenções contra: vírus, malwares, worms e trojans. Segue alguns métodos:

- Utilização do software de firewall: atua como uma camada adicional de proteção que atua como uma barreira entre a rede da empresa e a internet, contribuindo com o bloqueio de tráfegos maliciosos que possam conter malware.
- Uso de VPNs: tem o objetivo de fornecer conexões seguras entre redes remotas.
- Atualizações regulares de sistemas operacionais e aplicativos: tanto os sistemas quanto os aplicativos de todos os dispositivos da empresa devem permanecer atualizados. Esta medida auxilia na correção de vulnerabilidades que podem ser aproveitadas por malwares.
- Restringimento o acesso de usuários: montar uma cadeia de permissões que são fornecidas dependente de cada tipo de usuário ajudam a evitar que malwares se espalhem pela rede corporativa. Pode ser complementado com o uso de criptografia.
- Uso do software de detecção de intrusão: monitora a rede de forma constante a fim de localizar atividades suspeitas e as neutralizar, contendo possíveis ataques.
- Implementação de políticas de uso seguro: o estabelecimento destas direcionadas aos usuários conscientizam os mesmos a não clicarem em links maliciosos ou baixarem arquivos que comprometam a segurança da empresa.

6. Backup e Recuperação de Dados:

A organização deve fazer a adição de um processo de backup de recuperação de dados a fim de assegurar a disponibilidade e integridade de suas informações, que podem ser comprometidas a partir de falhas ou ataques à empresa. Com o estabelecimento de uma política de backup, os dados que precisam ser mantidos, independente da circunstância da rede, são identificados e salvos em um local reserva. Para isso, há os seguintes passos a serem seguidos:

- Selecionar a estratégia de backup adequada entre: backup completo, incremental e diferencial. A escolha da solução de backup adequada dependerá das necessidades da corporação.

- Escolher a solução de backup adequada entre: backup local, backup em nuvem, backup em fita e outras opções. A escolha da solução de backup adequada dependerá das necessidades da corporação e do tamanho dos dados a serem salvos.
- Testes regulares: a empresa deve testar regularmente o processo de backup para garantir que ele esteja disponível e operando corretamente para quando for necessário.
- Armazenamento seguro: os backups devem ser armazenados em locais seguros com usuários responsáveis para evitar a perda ou o roubo dos dados. O acesso aos backups deve ser restrito a pessoas autorizadas e o ambiente de armazenamento deve ser protegido contra ameaças físicas, como: incêndios, inundações e outras catástrofes possíveis.

7. Política de Senhas:

A empresa deve incrementar uma política de senhas fortes devido ao objetivo de proteger o acesso de usuários indesejados. A exigência dessas senhas se torna ainda mais correta caso tenham de ser complexas o suficiente para evitar tentativas de adivinhá-las, junto da necessidade de haver trocas regulares destas, garantindo que as senhas não sejam acostumadas ao uso por um longo período de tempo e fiquem suscetíveis a ataques.

Além disso, faz-se necessário a empresa demandar que os funcionários não compartilhem senhas ou outras informações sigilosas com outros usuários, dentro ou fora da empresa, e a não guardá-las em locais de fácil acesso.

8. Treinamento e Conscientização:

A Fictitious Company tem o dever de fornecer treinamento e conscientização aos seus funcionários e terceiros sobre suas políticas, suas normas e outros procedimentos, enfatizando a importância da segurança das informações.

9. Revisão e Atualização:

A PSI deve ser revisada e atualizada regularmente para garantir que esteja atualizada e eficaz para a proteção das informações da empresa e dos clientes.

Fictitious Company
Data: 8/05/2023