Empresa: Super atacado

Objetivo

Estabelecer os conceitos e as diretrizes da política de segurança da informação presentes no âmbito organizacional da Super Atacado, deixando a disposição dos colaboradores e envolvidos nas operações da empresa as regras que devem ser seguidas para preservação e gerenciamento de seus ativos. Assim, esta política deve ser entendida como uma declaração formal que deve ser seguida por todos os envolvidos nas operações da Super Atacado.

Segurança da Informação

A informação é um importante ativo para qualquer empresa e portanto deve se assegurar sempre seu gerenciamento e proteção. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento seja ele qual for. Porém este ativo possui uma enorme fraqueza que é a facilidade de acesso e propagação.

Toda e qualquer informação que está presente no âmbito digital ou físico sofre com a vulnerabilidade, portanto, é dever da Super Atacado seguir fielmente sua política de segurança da informação, a fim de prevenir e reduzir o máximo possível de problemas com seus dados, e claro, melhor gerenciamento destes.

Pilares da Segurança da Informação

- **Confidencialidade**

O Super Atacado visa sempre a garantia de que informações confidenciais só possam ser acessadas por pessoas autorizados para realizar essa atividade.

- **Integridade**

O Super Atacado visa garantir a exatidão e a completude das informações e dos métodos de seu processamento, e garantir sempre a integridade dos dados que possuem.

- **Disponibilidade**

O Super Atacado visa garantir que a informação esteja sempre disponível à solicitações por pessoas autorizadas, a fim de garantir o acesso eficiente a informação relevantes para a empresa.

Comitê de Segurança da informação

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial. A composição mínima deve incluir um colaborador de cada uma das áreas presentes na organização.

Aspectos Gerais

- As informações sobre negócios da Super Atacado são de propriedade exclusiva da empresa, não podendo sair do ambiente organizacional sem autorização formal.
- Quaisquer solicitação de acesso por pessoal não autorizado deve ter amplo consenso do Departamento da Segurança de Informação.
- Setores da empresa não podem ser acessados por pessoal não autorizado.
- O uso do sistema de gestão de estoque é exclusivo para o setor administrativo.
- As informações disponibilizadas na consulta de produtos em estoque só podem ser acessadas por pessoal autorizado.
- Documentos, planilhas e relatórios assim que impressos devem ser retirados o mais breve possível.
- Acesso a rede deverá ser feita somente pelo pessoal autorizado.
- Acesso a domínios que tendem a comprometer a segurança da organização devem ser evitados.
- O uso das redes sociais devem ser realizadas de maneira moderada, não devendo ser utilizadas para usos que não forem em prol da organização.
- Documentos pessoais e identificação devem ser mantidos em segurança.
- A utilização de dispositivos externos deverão ser previamente autorizados pelo Departamento de Segurança da Informação.

Violação da Política, Normas e Procedimentos de Segurança da Informação

A violação das atribuições expostas neste documento serão repassadas para o Departamento da Segurança de Informação por qualquer funcionário da organização, desde que seja justificada. O Departamento de Segurança de Informação será responsável pela análise da incidência, sendo que o responsável arcará com as consequências legais frutos de seu ato, caso confirmado.

Alguns exemplos de violação são:

1. Acesso a dados restritos
2. Circulação em locais sem autorização
3. Compartilhamento de dados a pessoas não autorizadas
4. Utilização de dispositivos externos sem autorização

Classificação do tipo de informação da Super Atacado

A classificação deve seguir os seguintes rótulos: Restrita, Confidencial, Interna ou Pública, considerando assim, as necessidades relacionadas ao negócio;

- Restrita: Informações essencialmente importantes para o desenvolvimento para atividades essenciais.
- Interna: Informações que auxiliam no desenvolvimento de atividade diárias.
- Pública: Acessível externamente, sem qualquer relação com os equipamentos internos na organização.

Responsabilidades

Permitindo que o repasse de violações ocorridas na organização seja feita por qualquer funcionário, estes devem:

- Conhecimento dessa política;
- Ações de acordo com essa política;
- Informar à segurança qualquer violação conhecida a essa política;
- Informar à segurança qualquer suspeita de problemas com essa política.

Na hierarquia encontrada, define-se:

- Administradores
  - Assegurar ações de conduta cabíveis ao código de conduta ética.
  - Informações sobre funcionários serão consideradas confidenciais.
- Departamento da Segurança da Informação
  - Mais alto nível de conduta ética;
  - Assegurar todas as ações consistentes com o código de conduta de um responsável pela segurança;
- Fornecedores
  - Acesso a informações previamente autorizadas
  - Deverá solicitar autorização de acesso a recursos internos desde que possa ser interpretada como questão de segurança
- Clientes
  - Sem acesso a qualquer equipamento interno da organização.
- Funcionários Gerais
  - Acesso a equipamentos autorizados.

Penalidades

As penalidades serão aplicadas conforme a classificação da importância da informação, juntamente ao Departamento da Segurança da Informação, podendo ser éticas ou disciplinares.

- Alta:
  a. Demissão
  b. Processo legal, de acordo com a legislação brasileira.
- Média:
  a. Descontos no salário
  b. Demissão
- Baixa::
  a. Suspensão (Sem remuneração)
  b. Advertência