Plano de Segurança da Informação

V.1.0

INTRODUÇÃO

Este Documento orienta e estabelece normas corporativas, para a proteção dos ativos de informação, e dita quais as responsabilidades dos envolvidos, devendo ser aplicada em toda a instituição. Este plano propõe um conjunto de ações estruturantes que alicercem e amparem a gestão da Segurança da Informação.

A empresa e a política de segurança

Todas as normas aqui estabelecidas serão seguidas por todos os funcionários, parceiros e prestadores de serviços. Ao receber uma cópia da Politica de Segurança, estará se comprometendo a respeitar todos os tópicos aqui abordados e estará ciente de todos os tópicos abordados por este plano.

O não cumprimento dessa política

O não cumprimento dessas políticas acarretará em sanções administrativas em primeira instância, podendo o colaborador ser desligado da organização de acordo com a gravidade da ocorrência.

DEFINIÇÕES

A gestão de ativos dever ser realizada pela Gerência de TI da , tendo como responsabilidades:

1. Inventário Identificação dos ativos no ambiente;

2. Gerenciamento de contrato de serviço ou garantia dos equipamentos;

3. Distribuição de pacotes e aplicativos remotamente;

4. Gerenciamento de atualizações homologadas para os equipamentos;

5. Monitoramento e rastreamento do ativo e suas atividades;

6. Resolução de eventuais incidentes e problemas com o ativo;

7. Aposentadoria, transição e migração de um ativo obsoleto para um novo ativo;

GESTÃO DE TRATAMENTO DE INCIDENTES

Para o tratamento adequado dos incidentes, espera-se um enfoque consistente e efetivo para gerenciar os incidentes relacionados a segurança da informação, ficando definido:

1. Terá uma equipe responsável pelo gerenciamento e tratamento de incidentes que

ocorrerem nos serviços prestados pela Gerência de TI. Essa equipe terá a missão de restaurar o serviço o mais rápido possível.

2. Com a implantação da Gestão de Ativos controlada pela Gerência de TI, será utilizado um portfólio que será um mapa contendo todos os ativos de TI e seus relacionamentos. Com isso será mais fácil e rápido a identificação dos incidentes, além de facilitar a descoberta da falha no serviço, ajudando a avaliar o impacto de uma atualização de software ou hardware.

3. Será implementada uma base de conhecimento garantindo que a gestão de incidente seja mais eficiente, pois com isso será possível armazenar erros conhecidos e suas soluções.

4. A Gerência de TI terá um monitoramento de disponibilidade que irá notificar de forma precisa sempre que houver alguma indisponibilidade, dessa forma, a equipe terá em tempo real as informações necessárias desse incidente.

GESTÃO DE RISCOS

A Gestão de riscos foi elaborada para garantir que os riscos envolvendo os ativos não possam paralisar o negócio da empresa. Com o levantamento dos ativos iremos descrever um plano para gerenciar e tratar os riscos já citados no plano de Segurança da Informação.

ANÁLISE DOS RISCOS E TRATAMENTO DOS ATIVOS DE HARDWARE E

SOFTWARE

Baseando-se na análise de riscos realizada na Política de Segurança da Informação onde foi identificado nos ativos abaixo uma alta probabilidade de ocorrência de incidente, loga abaixo foi definido as medidas de segurança preventivas:

1. Sistemas Operacionais Ameaças:

Sobreposição de identidade de usuário;

Erros de administração;

Propagação de software malicioso;

Acesso não autorizado.

Medidas Preventivas:

Manter o sistema operacional sempre atualizado.

Não usar conta com privilégios de administrador nas tarefas do dia a dia.

Utilizar bom anti-vírus e mantê-lo sempre atualizado.

Habilitar o firewall do sistema e criar um como barreira de entrada na rede interna .

Desabilitar o AutoRun do sistema.

Realizar treinamentos para orientar sobre bons hábitos de navegação e uso do computador.

Medidas Corretivas:

Criar uma rotina de auditoria para identificar quais os sites estão sendo acessados, tendo assim uma prova para aplicar uma advertência, e mesmo assim o habito de acessar conteúdos impróprios para o trabalho continuar, desligar o colaborador por justa causa.

2. Infraestrutura de Rede

Ameaças:

Manipulação de configuração de rede.

Erros de administração;

Interceptação dos pacotes;

Plano de Segurança da Informação

Bloqueio dos pontos de rede que não estiverem em uso.

Falta de energia elétrica

Medidas Preventivas:

A Gerência de TI deve distribuir pontos de rede de acordo com a necessidade de cada departamento, deixando sempre pontos extras para garantia. É necessário a instalação de nobreak para suportar os equipamentos ligados em caso de quedas de energia. Somente a Gerência de TI tem permissão para fazer quaisquer manutenção na infraestrutura de rede.

Medidas corretivas:

Fazer revisão e medição constante do uso dos recursos de rede interna e externa, fazendo as devidas correções encontradas. Em caso de incidentes, nenhuma ação deve ser tomada sem o conhecimento da Gerência de TI que é o departamento responsável.