POLITICA DE SEGURANÇA DA INFORMAÇAO

CONTEUDO

1 POLITICA DE SEGURANÇA DA INFORMAÇAO

1.1 Requisitos de Segurança da Informação

Uma definição clara dos requisitos para a segurança da informação na Security será acordada e mantida com os clientes internos do negócio e do serviço em nuvem, de modo que toda a atividade de segurança da informação seja focada no cumprimento desses requisitos. Requisitos estatutários, regulatórios e contratuais também serão documentados e inseridos no processo de planejamento. Requisitos específicos com relação à segurança de sistemas ou serviços novos ou alterados serão identificados em cada projeto.

E um princípio fundamental do programa de segurança da informação da Security, que os controles sejam implementados em razão da necessidade do negócio, e isso será comunicado regularmente a todos os funcionários por meio de reuniões de equipe e documentos informativos.

1.2 Quadro de configuração dos objetivos

Um ciclo regular será usado para a definição de objetivos de segurança da informação, para coincidir com o ciclo de planejamento orçamentário. Isso garantirá que um financiamento adequado seja obtido para as atividades de melhoria identificadas. Esses objetivos serão baseados em uma compreensão clara dos requisitos do negócio, informados pelo processo de revisão da administração, durante o qual as visões das partes interessadas podem ser obtidas.

Objetivos de segurança da informação serão documentados por um período, juntamente com detalhes de como eles serão alcançados. Estes serão avaliados e monitorados como parte das revisões de gestão para garantir que eles permaneçam válidos. Se forem necessárias emendas, elas serão gerenciadas por meio do processo de gerenciamento de mudanças.

Os controles de segurança da informação serão adotados, quando apropriado, pela Security. Estes serão revistos regularmente considerando o resultado das avaliações de risco e de acordo com os planos de tratamento de riscos de segurança da informação.

Além disso, controles aprimorados e adicionais de códigos serão adotados e implementados quando apropriado. A adoção desses códigos fornecerá garantia adicional aos nossos clientes e ajudará ainda mais com nossa conformidade com a legislação de proteção de dados.

1.3 Melhoria contínua da segurança da informação

A política da Security em relação à melhoria contínua é:

- Melhorar continuamente a eficácia dos controles de segurança da informação;
- Aprimorar os processos atuais para adequá-los às boas práticas;
- Aumentar o nível de proatividade (e a percepção da proatividade das partes interessadas) em relação à segurança da informação;
- Tornar os processos e controles de segurança da informação mais mensuráveis, para fornecer uma base sólida para decisões;
- Revisar métricas relevantes anualmente para avaliar se é apropriado alterá-las, com base nos dados históricos coletados;
- Obter ideias para melhoria por meio de reuniões regulares e outras formas de comunicação com as partes interessadas;
- Analisar ideias para melhoria nas reuniões regulares de gestão, a fim de priorizar e avaliar prazos e benefícios.

Ideias para melhorias podem ser obtidas de qualquer fonte, incluindo funcionários, clientes, fornecedores, equipe de TI, avaliações de risco e relatórios de serviço. Uma vez identificados, elas serão registradas e avaliadas em revisões administrativas.

1.4 Melhoria contínua da segurança da informação

A Security define a política em uma ampla variedade de áreas relacionadas à segurança da informação, descritas em detalhes em um conjunto abrangente de políticas que acompanha este documento.

Cada uma dessas políticas é definida e acordada por uma ou mais pessoas com competência na área específica e, uma vez formalmente aprovada, é comunicada ao público-alvo, dentro e fora da organização.

A tabela abaixo demostra as políticas individuais, resume o conteúdo de cada política e o público-alvo das partes interessadas.

Título da política	Areas endereçadas	Público-alvo
Política de Computação em Nuvem	Diligências, configuração, gerenciamento e remoção de serviços de computação em nuvem.	Funcionários envolvidos na aquisição e gerenciamento de serviços em nuvem
Política de Dispositivos Móveis	Segurança de dispositivos móveis, como laptops, tablets e smartphones, fornecidos pela organização ou pelo indivíduo para uso comercial e operacional.	Usuários de dispositivos móveis fornecidos pela empresa ou próprio dispositivo do funcionário
Política de Controle de Acesso	Registro de usuário e cancelamento de registro, acesso externo, revisões de acesso, política de senha, responsabilidades do usuário e controle de acesso ao sistema e ao aplicativo.	Funcionários envolvidos na configuração e gerenciamento do controle de acesso
Política Criptográfica	Avaliação de risco, seleção de técnica, implantação, teste e revisão de criptografia e gerenciamento de chaves	Colaboradores envolvidos na criação e gestão do uso de tecnologia e técnicas criptográficas
Política de Segurança Física	Areas de segurança local, segurança de documentos / equipamento e gerenciamento do ciclo de vida de equipamentos	Todos os funcionários
Política Antimalware	Firewalls, antivírus, filtragem de spam, instalação e verificação de software, gerenciamento de vulnerabilidades, treinamento de conscientização do usuário, monitoramento e alertas de ameaças, revisões técnicas e gerenciamento de incidentes de malware.	Funcionários responsáveis por proteger a infraestrutura da organização contra malware
Política de Segurança de Rede	Projeto de segurança de rede, incluindo segregação de rede, segurança de perímetro, redes sem fio e acesso remoto; gerenciamento de segurança de rede, incluindo funções e responsabilidades, registro e monitoramento e alterações.	Funcionários responsáveis por projetar, implementar e gerenciar redes
Política de Mensagens Eletrônicas	Envio e recebimento de mensagens eletrônicas, monitoramento de facilidades de mensagens eletrônicas e uso de e-mail.	Usuários de facilidades de mensagens eletrônicas
Política de Retenção e Proteção de Registros	Período de retenção para tipos de registro específicos, uso de criptografia, seleção de mídia, recuperação de registros, destruição e revisão.	Funcionários responsáveis pela criação e gestão de registros
Política de Proteção de Dados	Legislação, definições e requisitos de proteção de dados aplicáveis.	Funcionários responsáveis por projetar e gerenciar sistemas usando dados pessoais e aqueles que realizam algum tipo de tratamento aos dados pessoais.

Tabela 1 – Conjunto de documentos de política

1.5 Melhoria contínua da segurança da informação

As declarações de políticas feitas neste documento e no conjunto de políticas de suporte listadas na Tabela 1 foram revisadas e aprovadas pela alta direção da Security e devem ser cumpridas. O descumprimento dessas políticas pode resultar na tomada de medidas disciplinares de acordo com o processo interno da organização.

Perguntas relacionadas a qualquer política da Security deve ser abordada, primeiramente, pelo supervisor imediato do funcionário.