FACULDADE SENAC GOIÁS
GESTÃO DA TECNOLOGIA DA INFORMAÇÃO.

Lúcio de Souza Torres
Ordõnez Ribeiro
Vinicius Abadio
Jordy Alecssander

Governança de Tecnologia da Informação

GOIÂNIA/2019

Objetivo do Plano de Segurança da Informação

O Plano de Segurança da Informação deverá ser comunicada a todos a fim de que a política seja cumprida dentro e fora da empresa, quanto às normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

Deverá constar em todos os contratos da organização o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade. Todo incidente que afete a segurança da informação deverá ser comunicado imediatamente ao departamento responsável.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, assegurando que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.

Assim potencializar ao máximo, todos os meios que busquem garantir a total segurança dos processos praticados dentro da organização, assim como a segurança dos dados dos colaboradores e clientes, garantindo segurança contra possíveis delitos praticados por terceiros. Todo e qualquer usuário de recursos computadorizados da empresa tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

Plano de Segurança da Informação

1. Sistemas de Informação

A política de controle de acesso aos sistemas de informação deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios. O proprietário da aplicação deverá determinar regras apropriadas do controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários acessarem seus ativos, com o nível de detalhe e o rigor dos controles que reflitam os riscos de segurança da informação associados e que sejam considerados também os controles de acesso lógico e físico de forma conjunta.

2. Servidor Web

O Administrador do Servidor de aplicação é o responsável por conceder ou remover privilégios, criar ou excluir usuários, e atribuição de um nível de segurança aos usuários do sistema, de acordo com a política da organização.

Com a finalidade de eliminar os acessos não-autorizados ou diminuir as chances de sucesso das tentativas de invasão (internas ou externas). Os controles de acesso em sistemas de informação devem certificar que todos os acessos diretos ao sistema ocorram exclusivamente de acordo com as modalidades e as regras pré-estabelecidas, e observadas por políticas de proteção de dados.

3. Rede

Os usuários somente devem receber acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a fazer uso de acordo com a alocação departamental. A política seja formulada com relação ao uso de redes e serviços de rede, sendo que esta política esteja definida as seguintes especificações:

• Redes e serviços de redes que são permitidos de serem acessados;

• Monitoramento do uso dos serviços de rede;

• Requisitos de autenticação do usuário para acessar vários serviços de rede;

• Procedimentos de autorização para determinar quem tem permissão para acessar as redes e serviços de redes de acordo com o departamento que esteja alocado;

• Procedimentos e controles de gerenciamento para proteger o acesso a conexões e serviços de redes;

4. Base de Dados

O gerente do departamento de TI deverá liberar acesso aos colaboradores que devem ser os únicos a terem permissão para ler/editar as informações, obedecendo às atribuições de sua área de atuação. O objetivo da segurança lógica na Base de Dados é proteger os ativos de informações, sistemas ou programas de acesso indevidos e não autorizados. Somente os colaboradores credenciados e autorizados pelo Departamento de Segurança da Informação podem ter acesso aos dados armazenados. Os logs dos ativos de rede devem ser monitorados constantemente a fim de evitar acessos indevidos.

5. Antivírus

O software de antivírus deve ser atualizado mensalmente a fim de evitar possíveis invasões internas ou externas, e a qualquer indício de existência de vírus deverá interromper suas tarefas e comunicá-lo imediatamente ao Departamento de TI, que executará os procedimentos para a erradicação de vírus determinados no Plano de Política de Segurança da Informação. Mesmo em caso de falta de notificação por parte do usuário o antivírus envia automaticamente um e-mail de alerta para a área de TI passando todos os detalhes do fato ocorrido, facilitando uma ação rápida no intuito de evitar a propagação do problema.

Além dos programas que protegem a rede, todos os computadores devem possuir software de verificação de integridade, que detecta alterações nos arquivos de configuração e nos softwares e alertam ao usuário da possibilidade de existência de vírus.

6. Controle de acesso à documentação e ao código-fonte de programas

O acesso à documentação e ao código-fonte do programa deverá ser restrito. O acesso ao código-fonte de programas e de itens associados (como desenhos, especificações, planos de verificação e de validação) sejam estritamente controlados, com a finalidade de prevenir a introdução de funcionalidade não autorizada e para evitar mudanças não intencionais, bem como para manter a confidencialidade de propriedade intelectual da aplicação.