FACULDADE SENAC GOIÁS

LOJA VIRTUAL (E-COMMERCE)
SEGURANÇA DA INFORMAÇÃO

ELSON CRISTINO FARIAS
FABRÍCIO MOREIRA MACHADO
LUCAS EDUARDO
VINÍCIUS LOPES

Goiânia - GO
2020 / 1

FACULDADE SENAC GOIÁS
EIXO TECNOLOGIA
CURSO DE GESTÃO EM TECNOLOGIA DA INFORMAÇÃO

LOJA VIRTUAL (E-COMMERCE)
SEGURANÇA NA INFORMAÇÃO

Elson Cristino Farias
Fabrício Moreira Machado
Lucas Eduardo
Vinícius Lopes

Trabalho de conclusão do quinto período do curso de Gestão de Tecnologia da Informação apresentado como parte dos requisitos para a conclusão das disciplinas.

Goiânia – GO
2020 / 1

Política de Segurança da Informação e Comunicação do Projeto E-commerce

Controle de Versões

Versão	Data	Autor	Notas da Revisão
1.0	18/05/2020	Elson Cristino Farias	Criação do documento

1. Introdução

Esta política norteará a implantação de medidas de proteção que deverão ser aplicadas a toda e qualquer informação do Projeto E-commerce, independentemente de onde ela se encontre, com vistas ao resguardo da imagem e dos objetivos institucionais do Projeto.

Suas orientações devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos, para que o maior patrimônio do Projeto, a informação, tenha o grau de autenticidade, disponibilidade, confidencialidade e integridade exigidos.

2. Autenticação

Todos os colaboradores do Projeto autorizados pelo gerente do projeto, após a contratação, devem receber suas credenciais de acessos aos ativos do mesmo.

A criação das credenciais de acessos é solicitada pela gerencia do projeto, numa das seguintes condições:

1. Logo após a efetiva contratação do colaborador;
2. Após solicitação formal do Gerente do Projeto ou Coordenador responsável pela área do colaborador.

As credenciais de acessos estão ligadas a um ativo e definem os direitos de acesso de cada colaborador, de acordo com o cargo ocupado, função desempenhada, período de acesso e área em que esteja realizando suas atividades.

Um mesmo colaborador pode acessar um número diferenciado de ativos, possuindo credenciais correspondentes, cada qual os direitos de acesso necessários para o desempenho de suas atividades.

2.1. Política de Senha

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identificação do colaborador, evitando que uma pessoa se faça passar por outra.

Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

1. A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação;
2. É proibido o compartilhamento de login para funções de administração de sistemas;
3. As senhas deverão seguir os seguintes pré-requisitos:
    a) Tamanho mínimo de oito caracteres;
    b) Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais;
    c) Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge, etc.).
4. O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:
    a) Desligamento do colaborador;
    b) Mudança de função do colaborador;
    c) Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.

2.2. Política de E-mail

O e-mail é uma das principais formas de comunicação. No entanto, é, também, uma das principais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso.

1. O e-mail corporativo é destinado a fins profissionais, relacionados às atividades dos colaboradores;
2. Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;
3. É proibido abrir arquivos com origens desconhecidas anexadas a mensagens eletrônicas;
4. É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo "corrente", campanhas ou promoções;
5. É proibido enviar qualquer mensagem por eletrônicos que torne o Projeto vulnerável a ações civis ou criminais;
6. É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
7. Produzir, transmitir ou divulgar mensagem que:
    a) Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malware;
    b) Contenha arquivos com código executável (.exe, .cmd, .pif, .js, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    c) Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    d) Vise obter acesso não autorizado a outro computador, servidor ou rede;
    e) Vise vigiar secretamente ou assediar outro usuário;
    f) Vise acessar informações confidenciais sem explicita autorização do proprietário;
    g) Tenha conteúdo considerado impróprio, obsceno ou ilegal;
    h) Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
    i) Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
8. O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:
    a) Não contrariar as normas aqui estabelecidas;
    b) Não interferir, negativamente, nas atividades profissionais individuais ou de outros colaboradores;
    c) Não interferir, negativamente, no Projeto e na sua imagem.

2.3. Política de Acesso à Internet

O ativo corporativo de acesso à internet do Projeto é destinado para finalidades direcionadas ao projeto e restritas às atividades dos colaboradores, podendo ser para fins pessoais dentro de critérios de razoabilidade e responsabilidade.

Os termos e Condições de Uso e a Política de Privacidade dos sites acessados devem ser lidos antes de qualquer inscrição ou atividades nos sites publicados na internet, quando aplicável.

Não é permitido aos colaboradores no uso dos ativos corporativos de acesso à Internet:

1. Visualizar, utilizar, armazenar, divulgar, repassar e imprimir qualquer material, conteúdo, serviço ou recurso que não sejam compatíveis com as atividades do Projeto, e ainda:
    a) Com fins de propaganda política local, nacional ou internacional;
    b) Arquivos executáveis, com a extensão .exe, ou equivalentes, não autorizados pelo Projeto;
    c) Sites contendo pornografia, pedofilia, incitação ao terrorismo ou qualquer outro conteúdo que atente contra as leis vigentes e a ordem pública;
    d) Jogos on-line ou stand-alone;
    e) Programas de compartilhamento de arquivos (tais como BitTorrent, por exemplo);
    f) Programas ou plugins de camuflagem de navegação, deleção de histórico de navegação, de desvio de Proxy e/ou tunelamento de navegação;
    g) Programas de comunicação instantânea não autorizados;
2. Efetuar o upload indevido de qualquer conteúdo de propriedade do Projeto.
3. Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades em sistemas do Projeto;
4. Tentar indevidamente obstruir, desativar ou alterar os controles de segurança e os seus parâmetros estabelecidos nos ativos do Projeto;

O fato de um site não estar bloqueado pela direção do Projeto, não significa que ele pode ser acessado. Todo colaborador deve observar às restrições estabelecidas por este documento no uso dos ativos corporativos.

No caso de um site bloqueado, cujo conteúdo está em conformidade com as regras e diretrizes deste documento, o colaborador pode solicitar formalmente a liberação de acesso junto a direção. O pedido deve conter o endereço do site e

o motivo de acesso ao site.

3. Política de uso de Estação de Trabalho

As estações de trabalho devem permanecer operáveis durante o maior tampo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

1. Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;
2. É de responsabilidade do colaborador do equipamento zelar pelo mesmo, mantendo-o em boas condições;
3. É proibida a instalação de software ou sistemas nas estação de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe do Projeto;
4. É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe
5. É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe do Projeto;
6. As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas;
7. As estações de trabalho devem permanecer bloqueadas nos períodos de ausência do colaborador;
8. Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina;
9. Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;
10. É proibido o uso de estações de trabalho para:
    a) Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
    b) Burlar quaisquer sistemas de segurança;
    c) Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
    d) Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    e) Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
11. As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na dele. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

4. Política Social

Nós seres humanos, temos o grande privilégio de sermos sociáveis, mas muitas vezes quando o assunto é segurança, se torna uma desvantagem. Por isso devemos observar os tópicos a seguir:

1. Não fale sobre a política do Projeto com terceiros ou em locais públicos;
2. Não revele sua senha para ninguém. Os colaboradores da equipe em hipótese alguma pedirá a sua senha;
3. Não digite suas senhas ou usuários em máquinas que sejam de terceiros, especialmente que não sejam do Projeto;
4. Só deverá ser aceito suporte técnico de um membro de nossa equipe previamente apresentado e identificado.
5. Nunca execute procedimentos técnicos cujas informações tenham chego por e-mail;
6. Informe a equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

5. Vírus e Códigos Maliciosos

Esta política se aplica a todos os colaboradores do Projeto, todos esses colaboradores serão tratados nesta política como usuários.

1. Diretrizes Gerais e Infraestrutura:
    a) Todos os equipamentos que têm a funcionalidade de servidores, tanto físicos quanto virtuais, equipamentos de mesa (PCs), dispositivos móveis e de segurança da informação, devem estar protegidos com sistemas de proteção contra softwares maliciosos e serem atualizados periodicamente, conforme recomendação de disponibilização do fabricante;
    b) Devem ser estabelecidos procedimentos que visem os controles de detecção e combate a softwares maliciosos;
    c) Caso o usuário perceba que no seu equipamento de trabalho os sistemas de proteção, como antivírus e firewall, não estejam instalados ou funcionando adequadamente, este deve entrar em contato com a central de serviços para as devidas providências;

d) Apenas a área técnica do Projeto deve realizar instalação de software ou aplicativos no ambiente tecnológico do Projeto, com a finalidade de manter o controle, evitando a introdução de vulnerabilidades e possível vazamento de informações, perda de integridade ou outros incidentes de segurança da informação, além da violação de direitos de propriedade intelectual;
e) Os sistemas de proteção contra software maliciosos devem ser instalados com controles que não permitam alteração de sua configuração de direitos de propriedade intelectual;
f) Os equipamentos não homologados pela área técnica do Projeto na rede local na devem ser utilizados, conformes Política de Ativos de Dispositivos Móveis, evitando a entrada de possíveis infecções por equipamentos nocivos ao ambientes tecnológicos do Projeto.

2. Diretrizes de Tratamento de Arquivos, Software e Aplicativos:
    a) Todos os arquivos recebidos por meio de redes, em qualquer mídia de armazenamento, correio eletrônico, arquivos baixados ou em páginas web, devem ser verificados automaticamente quanto à presença de códigos maliciosos, antes de serem utilizados;
    b) Para minimizar o risco de infecção por software maliciosos, os usuários devem usar, exclusivamente, softwares homologados, licenciados e instalados pela área técnica do Projeto.
3. Analise de Vulnerabilidade:
    a) Periodicamente devem ser realizadas analises de vulnerabilidades de softwares, aplicativos e infraestrutura que suportam os processos críticos do ambiente tecnológico do Projeto;
    b) A resposta às vulnerabilidades críticas detectadas nos sistemas e ambientes do Projeto deve ser tratada imediatamente pela equipe de Resposta a Incidentes, conforme descrito na Política de Resposta a incidentes de segurança da informação;
    c) Deve ser mantido e atualizado o procedimento de análise, testes e implementação de contramedidas que visem reduzir vulnerabilidades, que possam ser exploradas por códigos maliciosos;
    d) Caso não seja possível realizar os testes adequados para implementar a correção, deve ser realizada uma análise de risco associado a correção, considerando experiências de outros ambientes tecnológicos e aguardar um período mais longo para a implantação;
    e) Deve ser definido o procedimento de obtenção de informações relativas aos códigos maliciosos e vulnerabilidade e ao prazo para a reação as notificações de potenciais vulnerabilidades técnicas relevantes.
4. Atualização e Monitoração
    a) A área técnica do Projeto é responsável por gerir e manter os ativos de softwares vigentes com as correções mais recentes, além de suportar os mecanismos de controle e combate a software maliciosos, mantendo estes e aqueles com as licenças, e devidas correções atualizadas;
    b) Regularmente, a área técnica do Projeto deve apresentar ao Comitê de TI, relatórios com as tentativas e ataques e ações tomadas, os maiores ofensores, equipamentos desatualizados ou vulneráveis, equipamentos gerenciáveis e não gerenciáveis, controle das licenças utilizadas e disponíveis e prazo de licenças a vencer, entre outros;
    c) Os relatórios específicos de respostas a incidentes relacionados a softwares maliciosos devem apresentar correlação de informação e detalhes, que viabilize ações corretivas e preventivas;
    d) A área técnica do Projeto deve fazer a monitoração e análise constante do tráfego da rede local, de forma que se identifiquem, entre outras, ameaças relativas a tráfego malicioso ou atividades incompatíveis com as políticas de uso e segurança da rede, viabilizando a tomada de providências.
5. Ações disciplinares
    a) A intenção de introduzir ou espalhar software maliciosos no ambiente tecnológico do Projeto poderá acarretar sanções administrativas disciplinares e/ou contratuais aos seus respectivos usuários, sem prejuízo das responsabilizações nas esferas civil e criminal.

6. Equipe de Segurança

1. Formada por equipe multidisciplinar de colaboradores, com o objetivo de deliberar a respeito de assuntos relacionados à Segurança da Informação do Projeto E-commerce. Assim deve:
    a) Implementar mecanismos de segurança com base no valor associado às informações e ao impacto oriundo da perda dessas informações;
    b) Promover instrução relacionada à Segurança da Informação;
    c) Acompanhar e analisar as transações e alterações relacionadas à Segurança da Informação, para fins de rastreamento e auditoria;
    d) Realizar, periodicamente, monitoramento e auditoria de segurança no ambiente tecnológico;
    e) Priorizar medidas preventivas, em detrimento de controles reativos;
    f) Viabilizar monitoração e controle com soluções técnicas que não dependam de processos manuais ou não estejam sujeitas a erros humanos.

6.1. Membros da Equipe Técnica

Nome	E-mail	Ramal	Celular
Elson Cristino Farias	*********	**	********
Vinícius Lopes	*********	**	********

6.2. Membros da Equipe de Segurança

Nome	E-mail	Ramal	Celular
Lucas Eduardo	**********	**	********
Fabricio Moreira	**********	**	********
Leandro Soares	**********	**	********