GTI - V - NOTURNO
ARTHUR OLIVEIRA, ISADORA SERRANO, JOÃO MOITA MATHEUS FERREIRA

GOVERNANÇA EM TI
POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Trabalho realizado como tema do projeto Integrador
do componente curricular de Governança em TI,
Ministrado pelo professor: **Marcelo Faustino**

Goiânia
2018

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

1.0 INTRODUÇÃO

A empresa JAMI (João Moita, Arthur Oliveira, Matheus dos Santos Ferreira e Isadora Serrano), consiste em uma loja virtual que opera em diversos departamentos, a empresa recebe as iniciais de seus proprietários, sendo estes profissionais atuantes da área de Tecnologia da informação, voltada ao comércio e segurança. O presente documento especifica as regras e diretrizes que devem ser seguidas quanto a utilização da Loja Virtual.

As diretrizes foram elaboradas para especificar um modelo ideal de segurança na utilização e manutenção da loja virtual.

PROFISSIONAIS RESPONSÁVEIS PELA POLÍTICA DE SEGURANÇA			
Nome	E-mail	Telefone	Cargo
Matheus dos Santos	matheus19gyn@gmail.com	(11)4002-8922 (62)99152-9875	Analista de Rede, Auditor de Software e Projetista
João Moita Manrique	joaomoitamanrique@gmail.com	(62)99999-9999	Programador, Analista de Sistemas
Arthur Oliveira	arroiseeu@gmail.com	(62)99837-0293	Programador, Gestor de negócios
Isadora Serrano Fideliz	isadora@gmail.com	(62)99870-0988	Advogada, Gestora de negócios

2.0 OBJETIVO

Este documento tem como objetivo a especificação das diretrizes e normas para uma melhor gestão e proteção das informações, assim como os ativos relacionados a empresa JAMI. A fim de estabelecer uma política da informação, que visa minimizar ou eliminar os riscos existentes a integridade, disponibilidade e usabilidade dos sistemas propostos.

A segurança das informações deve ser algo primordial para a empresa, esse documento tem como principal objetivo manter esse fundamento, estabelecendo as

seguinte metas: implementar uma melhoria contínua de seus processos internos, controle de acesso, rastreabilidade das operações, facilidade nos processos de gestão e integridade das informações.

As políticas aqui estabelecidas passam a ser válidas a partir:

- Apresentação e esclarecimento das políticas de segurança a todos os stakeholders;
- Assinatura dos membros da organização.

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

3.0 CONFIABILIDADE

A Loja Virtual possui um servidor próprio, hospedado em nuvem, e conta com vários protocolos de segurança (HTTPS, VPN, etc), de autenticação, criptografia entre outros recursos que contribuem para a segurança no acesso à loja. Como a conexão pode ser realizada ponto a ponto e a loja possui uma certificação de confiança, a probabilidade de que o cliente tenha seus dados expostos é praticamente zero. O Serviço não utiliza cookies, o que significa que o usuário que utilizar a loja não recebera spams a todo o momento ofertando produtos desejados.
Todos os dados de acessos e informações são armazenados em um servidor de backup, que contribui para uma maior segurança e redundância das informações.

4.0 INTEGRIDADE

A empresa conta com auto padrão de qualidade de segurança da informação para garantir de que a informação que chegue ao cliente esteja de acordo com a que foi implementada na Loja Virtual, estando em seus estado original. Um backup que é realizado semanalmente para garantir a persistência dos dados.
O sistema é automatizado com os itens de estoque, ou seja, quando um produto do portfólio estiver em falta, este é retirado do site, ou é exibido com uma mensagem de alerta sobre a mercadoria.

5.0 DISPONIBILIDADE

Como o sistema consiste em uma Loja Virtual, este é hospedado em um servidor, e pode ser acessado de qualquer navegador, tanto de notebooks, desktops e também de smartphones, desde que tenham acesso à internet e um navegador.

A Loja Virtual apesar de ter um portfólio limitado de mercadorias, não possui uma quantidade específica para usuários cliente, seus produtos está disponível a todos para visualização e estes podem fazer a aquisição do que desejar, através de um cadastro no próprio site da Loja.

6.0 AUTENTICIDADE

6.1 SEGURANÇA DE ACESSO:

ADMINISTRADOR:

Cada usuário administrador da loja possui um login e senha únicos, estes são previamente cadastrados pelo administrador sênior da Loja, os dados são exclusivos para cada usuário, portanto esse não deve compartilhá-los com outras pessoas.

FUNCIONÁRIO:

Assim como o administrador, o funcionário possui uma chave de acesso única, essa é de uso exclusivo de cada funcionário, e é criada pelo administrador assim que o funcionário é registrado.

CLIENTE:

O cliente deve possuir uma conta criada antes de efetuar uma compra, caso não tenha, esse pode se cadastrar no ato da compra. A forma como essa conta de acesso será administrada (compartilhada ou não) fica a critério do cliente, porém recomenda-se que a conta seja individual.

6.2 NÃO REPÚDIO

Uma vez que um funcionário ou cliente é cadastrado, este recebe um login para autenticação e uso do sistema, onde todas as suas operações realizadas ficam registradas em sua sessão de acesso. Caso alguma operação tenha sido realizada e o usuário negue que tenha sido ele a realizá-la, uma perícia rápida é realizada, sendo constatado que as operações foram realizadas na sessão em que esse usuário se autenticou, esse será responsável pelas ações, uma vez que o login realizado tenha sido de sua autoria.

Recomenda-se que as senhas sejam atualizadas periodicamente, ou sempre que houver suspeita de vazamento de dados de acesso.

Para a criação de senhas, recomenda-se a utilização de senhas que contenham as seguintes especificações:

- Mínimo seis caracteres;
- Letras maiúsculas e minúsculas, números e caracteres especiais;
- Evitar senhas genéricas ou pessoais (nomes pessoais, idade, nome de ocupação, etc.).

6.3 SEGURANÇA DOS DADOS:

Em momento algum os dados de login do cliente serão solicitados pelos funcionários da Loja Virtual, ficando este princípio como resguarda da segurança da Loja Virtual.

Os dados do cliente são de responsabilidade exclusiva deste, não podendo os funcionários ou administrador executar qualquer operação em seu nome.

7.0 RESPONSABILIDADES DOS STAKEHOLDERS

Os principais usuários do sistema são os funcionário, que realizam a gestão deste, e o cliente que efetua suas compras, o usuário responsável pela gestão geral, manutenção do site e outros assuntos é o administrador, as funções, responsabilidades e restrições destes usuário são descritas a seguir:

ADMINISTRADOR:

- Usuário responsável pelo cadastro de funcionários, produtos e formas de pagamento;
- Possui a função de administrar as operações dos funcionários e clientes;
- Responsável pela gestão de manutenção e novas atribuições na Loja Virtual;
- Responsável pela manutenção dos produtos da Loja (Inserção e Exclusão);
- Não pode se cadastrar para compra produtos da Loja Virtual.

FUNCIONÁRIO:

- Responsável pela manutenção (alteração e upgrades) dos produtos na Loja;
- Responsável pelo controle de vendas;
- Possui a função de administrar o cadastro de clientes;
- Pode se cadastrar como cliente para adquirir um produto da Loja.

CLIENTE:

- Único usuário que pode se cadastrar no sistema;
- Pode efetuar compras na Loja;
- Pode escolher o meio de pagamento desejado.

8.0 PERMISSÕES

1) Todo o usuário deve se autenticar para utilizar o sistema;
2) Somente o cliente pode se cadastrar no sistema;
3) Os produtos da loja são visíveis a todos os que entram no site;

4) Essa política de segurança da informação é disponibilizada ao usuário, cliente e funcionário, no momento do cadastro, se este concordar com os termos aqui presentes o cadastro é efetivado, caso não concorde, o cadastro não terá prosseguimento;
5) Os boletos, comprovantes de pagamento, documentações, entre outros arquivos, serão encaminhados ao e-mail que o usuário cadastrou no sistema;
6) Qualquer cliente é livre para escolher a forma de pagamento que o sistema disponibiliza.

9.0 RESTRIÇÕES

1) Somente o administrador possui acesso e pode modificar o código fonte da Loja Virtual;
2) Todo os produtos da loja podem ser vendidos em uma quantidade de no máximo dez unidades;
3) Os meios de pagamento se limitam a cartões de crédito, débito e boleto bancário;
4) As compras só podem ser efetuados após um login de identificação;
5) Os dados de login são únicos para cada usuário, estando a exposição deste exposto as penalidades aqui expressas;

10.0 RECOMENDAÇÕES

1) Para garantir uma maior integridade e disponibilidade dos dados, deve ser realizado um backup semanalmente de todas as operações (cadastros, atualizações, compras, pedidos, etc.) realizadas na loja virtual;
2) Deve ser realizado um registro de todos os ativos da Loja Virtual, tanto físicos (hardware, equipamentos, materiais, etc) quanto lógicos (softwares, códigos, documentos virtuais, etc);
3) Realizar cópias deste documento: Políticas de Segurança, e manter sempre um impresso, para esclarecimento de dúvidas, comprovante e documentação;
4) Como descrito anteriormente, realizar uma atualização periódica das senhas, conforme descrito no item **6.2**.
5) Sempre que o usuário terminar de utilizar a loja, faça o logoff, para encerrar sua sessão, para evitar que outros usuário possam realizar operações em sua conta, e assim evitando possíveis constrangimentos, conforme descrito no item: Não Repúdio;
6) Verificar se a rede em que o usuário está, wi-fi ou LAN, é de fonte confiável e segura, antes de acessar o site da Loja Virtual;
7) Sempre verificar se onde no campo de endereço do link da Loja Virtual aparece o protocolo de conexão segura HTTPS, caso não, opte por reiniciar o navegador e abrir uma nova sessão;

8) Não aceite a ajuda de estranhos para realizar suas operações na Loja Virtual;
9) Não deixe seus dados de login salvos no navegador, opte sempre por nunca salvar os dados de login, para logar automaticamente, sendo que outros usuários podem acessar a máquina e realizar operações indesejadas.

11.0 PENALIDADES

1) Os dados de acesso ao site, usuário e senha, é de responsabilidade individual, caso algum desconhecido logue com o acesso de terceiros a administração do site não se responsabiliza pelas operações realizadas;
2) Sendo identificado um acesso ilegal ao site (utilização de dados de terceiros para login), esse mesmo poderá responder processo, sob pena de multa por danos morais;
3) O acesso ao código fonte é exclusivo do administrador e de outros por esse autorizados. Caso algum terceiro tenha acesso ao código sob desconhecimento do administrador e o mesmo: visualize, modifique, copie ou exclua, responderá processo sob pena de prisão, multa por danos morais e consequências causadas, sendo essa sanção definida pelo juiz criminalista;
4) Caso algum funcionário faça alguma divulgação não autorizada da Loja Virtual, obtenha acesso a arquivos não autorizados e copie, visualize ou os modifique, esse cumprirá sanção administrativa, e dependendo da gravidade o mesmo poderá responder processo perante a lei;
5) É proibida a divulgação de informações pessoais (dados de login, compras realizadas, entre outros) do cliente a terceiros, o descumprimento dessa norma, acarretará em processos perante a lei, por quebra do direito do consumidor, e sanção administrativa sob pena de demissão e multa por quebra de sigilo e violação dos direitos do cliente;
6) O cliente que fornecer informações enganosas no momento do cadastro, dependendo da gravidade das consequências futuras, poderá responder na justiça por falsificação de identidade ou quaisquer outros dados informados de forma enganosa.