Padrão de Segurança para Aplicações

Marketing

Conteúdo

1. Segurança HotSite Clientes

Passo 1 – Acesso ao Site

1. *Tem que ser HTTPS para:*
    a. *Autenticação,*
    b. *Cadastro ou*
    c. *Utilização de dados considerados confidenciais (ex. CPF, MSISDN, Nome Completo, Endereço Completo e outros que possam ser passíveis de fraudes).*
2. *Criação/Registro do Domínio*
    a. *O Domínio do Site deve ser comprado e registrado pela Claro, mas em algumas situações a infra-estrutura do site ficará na infra-estrutura do parceiro, desta forma se for um domínio que remete o nome da Claro e for de interesse da Claro, este deverá ter em contrato que ao final da prestação dos serviços o parceiro deverá transferir o domínio para o gerenciamento da Claro.*
3. *Solicitação de certificado (HTTPS)*
    a. *A geração de certificado para implementação no site é de responsabilidade da empresa/CNPJ que registrou o domínio, caso o domínio seja transferido para outra empresa/CNPJ a emissão do novo certificado passa a ser da mantenedora do domínio;*
    b. *Existem algumas situações onde a Claro é a dona de um domínio, porém a infra-estrutura estará no ambiente do parceiro, desta forma a geração do certificado é de responsabilidade da Claro, porém o Parceiro fica responsável de custódia do Certificado, sendo responsável por qualquer incidente de segurança que possa acontecer, se comprovado o vazamento de informações através de falhas de processo no Parceiro. Este é um item, cuja responsabilização do Parceiro deverá ser prevista em Contrato, inclusive apontando quais sanções e multas a serem aplicadas.*
4. *Transferência de Domínio*
    a. *Em todos os contratos definidos, quando for de interesse da Claro, deve se ter uma clausula informando que ao final do contrato com o parceiro o domínio deverá ser transferido para o CNPJ da Claro.*

Passo 2 – Processo de Cadastro do Usuário/Cliente no Site

1. *Validação se é ou não cliente Claro*
    a. *Integração com Serviços/Plataformas da Claro para validação se é ou não cliente, por exemplo, através do número do CPF ou MSISDN;*
        i. *Sempre deverá acontecer através de Link Dedicado, VPN ou HTTPS com algum nível de autenticação;*
    b. *Troca de arquivos com dados cadastrais de clientes para o parceiro para validação se é ou não cliente;*
        i. *A troca de arquivos sempre deverá acontecer através de protocolos e ferramentas que garantam a confidencialidade dos dados como SFTP, VPN ou Connect Direct, sempre com algum nível de autenticação e validação dos dados trafegados pela equipe de Segurança da Informação Corporativa.*

2. *Termo de Aceite*
    a. *Sempre que for disponibilizado um serviço para usuários e clientes deverão ser disponibilizados documentos que reportem:*
        i. *Termo de Aceite;*
        ii. *Política de Privacidade;*
        iii. *Política de AntiSpam (em caso de serviços de Email e SMS);*
        iv. *Contrato de Prestação de Serviço;*
        v. *Documento de Regras de Utilização;*
        vi. *Criar uma área de Denúncia;*
        vii. *Termo de Responsabilidade sobre a utilização;*
        viii. *Entre outros documentos que podem ser discutidos conforme a necessidade.*
3. *Dados Cadastrais*
    a. *Processo de Cadastro pelo usuário/cliente*

i. *Deverá ter interface de cadastro para a realização do Auto-Cadastro pelo cliente/usuário;*
ii. *Ao final do Cadastro do usuário/cliente a aplicação deverá realizar a validação de Captcha impedindo o cadastro de usuários em massa através de robôs;*
iii. *O cadastro sempre deverá ser confirmado a partir de um código enviado para o celular do cliente. Ao receber o código o cliente terá que digitá-lo no site.*

b. *Entrada/validação de dados*
   i. *Validação de MSISDN*
   ii. *Validação de Critérios como cliente ou não Claro*

c. *Armazenamento*
   i. *Armazenamento criptografado de dados cadastrais de clientes ou controle de acesso restrito aos dados, porém com geração detalhada de logs de consulta dos dados, seja por meio da aplicação ou comandos executados diretamente em banco dados sempre coletando e registrando os dados de log:*

d. *Gestão*
   i. *A empresa deverá tratar e apresentar os procedimentos relacionados ao processo de backup e restore em casos de incidente, bem como os SLAS necessários;*
   ii. *A empresa deverá tratar e apresentar os procedimentos relacionados ao Gerenciamento de Identidades dos usuários.*

e. *Manuseio*
   i. *A empresa deverá tratar e apresentar os procedimentos relacionados à integridade, confidencialidade e disponibilidade das informações.*

f. *Expurgo*
   i. *A empresa deverá tratar e apresentar os procedimentos nas questões relacionadas ao expurgo dos dados, tanto os armazenados de forma on-line quanto off-line;*
   ii. *Ao término de um Contrato de Prestação de Serviços, deve-se prever que todas as informações geradas pelo Parceiro sejam disponibilizadas para a nossa empresa e garantido que não haja nenhum tipo de retenção de informações de nossos Clientes/Processos desde que essa retenção não esteja descrita como necessária em CONTRATO.*

4. *<u>Processo de Cadastro de Login</u>*
   a. *De preferência a aplicação deverá estar integrada ao "Senha Única" da Claro para os clientes Brasil já com validação do tipo de login;*
   b. *Caso não tenha integração deverá ter a definição do tipo de login que será utilizado, nome, email, MSISDN, CPF, CNPJ etc;*
   c. *É necessária a validação do login antes da criação;*
   d. *É necessário que o usuário/cliente cadastre uma conta de email ou celular secundário no qual possa receber uma mensagem com o lembrete de seu login.*

5. *<u>Processo de Cadastro de Senha</u>*
   a. *De preferência a aplicação deverá estar integrada ao "Senha Única" da Claro para os clientes Brasil;*
   b. *Caso não seja integrado ao "Senha Única" o parceiro não deverá armazenar a senha do usuário, apenas seu hash;*
   c. *Em caso de armazenamento de senhas, estas devem ser armazenadas de forma criptografada, a chave de criptografia deve ser gerenciada pela aplicação e a utilização de um HSM para o armazenamento da Chave Privada é fortemente recomendada devido a criticidade da informação que será tratada;*
   d. *O Cadastro da Senha deverá atender as Políticas de Senha da Claro que contemplam:*
      i. Mínimo de 8 caracteres(sendo números, letras e caracteres especiais);
      Salvo os casos em que a senha deverá ser digitada através do teclado de um celular!
      ii. A senha inicial deve expirar no primeiro acesso (criação e reset da senha);
      iii. A nova senha não poderá ser igual às últimas 12 (doze) senhas utilizadas;
      iv. O período de expiração da senha deve ser de 90 (trinta) dias à partir da data de sua criação;
      v. Todo e qualquer acesso deve ser bloqueado após 5 (cinco) tentativas incorretas;
      vi. Não será permitida a simultaneidade de sessões de um mesmo usuário.

e. *A aplicação deverá contar com sensor de dificuldade da senha que vai mudando de cor conforme a dificuldade da senha aumenta ou diminui (vermelho: senha fraca, amarela: segurança média e verde: senha segura);*
f. *É necessário que o usuário/cliente cadastre uma conta de email ou celular secundário no qual possa receber uma mensagem com uma nova senha para acesso ao sistema.*

Passo 3 – Autenticação para acesso

1. *Processo para tratar "Autenticação"*
   a. *Teclado Virtual e Captcha*
      i. *A utilização de teclado virtual também é uma importante forma de garantir que a senha do cliente não será roubada através de keyloggers;*
      ii. *No processo de Autenticação o usuário deverá entrar com login e senha, após 3 tentativas incorretas deverá ser apresentado ao usuário o Captcha como forma de inibir a utilização de robôs;*
   b. *2º Fator de Autenticação*
      i. *Se for uma aplicação considerada Crítica pelas áreas de Segurança da Claro além da utilização de HTTPS na tela de autenticação e login e senha o cliente deverá entrar também com uma 2º senha adicional enviada por SMS;*
   c. *Histórico de Acessos*
      i. *A aplicação deverá ter uma área informativa para o cliente onde deverá ser apresentado o histórico dos últimos acessos com data, hora e endereço ip de conexão.*

2. *Processo para tratar "Esquecimento de login"- Lembrar Login*
   a. *A aplicação deverá ter processo para lembrar o login cadastrado, para isso ele deverá ter cadastrado uma "dica" no momento do cadastro de sua conta e também uma conta adicional de email ou celular para receber a mensagem com a dica;*
   b. *Para que a dica seja enviada o usuário/cliente deverá confirmar alguns dados que deverão ser definidos após o fechamento dos campos de cadastro.*

3. *Processo para tratar "Esquecimento a senha" – Resetar a Senha*
   a. *A aplicação deverá ter processo para resetar a senha do usuário em caso de esquecimento, para isso ele deverá ter cadastrado uma conta adicional de email ou celular para receber a mensagem com a dica;*
   b. *Para que a nova senha seja enviada o usuário/cliente deverá confirmar alguns dados que deverão ser definidos após o fechamento dos campos de cadastro;*
   c. *A nova senha deverá estar com status de expirada e sua alteração deverá acontecer obrigatoriamente no primeiro acesso.*

4. *Atualização de Dados Cadastrais*
   a. *A atualização de dados cadastrais de usuários/clientes só deve acontecer por meio de acesso do próprio cliente ao sistema se necessário a utilização de um 2º fator deverá ser aplicada.*

5. *Processo para tratar "Troca de senha"*
   a. *A aplicação deverá disponibilizar um serviço de troca de senha para o usuário/cliente. Este poderá alterar sua senha após acesso autenticado na aplicação onde entrará com senha atual, nova senha, confirmar nova senha e captcha.*

Passo 4 – Utilização do Serviço

1. *Armazenamento/Compartilhamento/Disponibilização de Conteúdo*
   a. *Fatores como autenticidade, integridade e legalidade de conteúdos devem ser levados em consideração caso a aplicação permita o armazenamento de conteúdo protegidos legalmente como:*
      i. *Vídeos, filmes, imagens, músicas etc*
      ii. *Conteúdos pornográficos ou pedofilia etc*

Este recurso pode trazer problemas jurídicos tanto para o usuário como para Claro;

b. *Este tipo de serviço deve ser contar com a possibilidade de monitoramento e permitir rastreamento do usuário em caso de Mandatos Judiciais e quebra de Sigilo.*

2. *Entrada de comentários*
   a. *Toda aplicação que trabalhar com recursos de blog devem contar com Moderadores (humanizados) que possam ter critérios na autorização ou não de divulgação do comentário;*
   b. *Deve contar com aplicações automatizadas que gerenciem listas negras de palavras ou arquivos/imagens.*
3. *Consulta/Utilização de serviços de outros Sites*
   a. *Toda aplicação que contiver o compartilhamento de dados de serviços gerenciados por outros sites como senhas, por exemplo, devem ter alertas para os usuários quanto aos riscos existentes neste processo e a importância dos cuidados que deverá ter com as credenciais de acesso ao serviço.*
4. *Utilização de Serviços Online*
   a. *Se o serviço disponibilizar aplicações on-line como antispam, antivírus, ferramentas de backup ou outros, deverão ser disponibilizados ao usuário/cliente manuais de instalação, configuração, atualização e utilização no idioma do cliente;*
   b. *Para que este tipo de serviço entre em produção para o cliente é necessário que antes passe pelas validações/testes de segurança da Claro.*
5. *Download de Aplicações*
   a. *Para disponibilização de instalações/clients para que o cliente instale em sua estação é necessário que o "client" seja identificado e que seja certificado e assinado digitalmente por uma certificadora reconhecida mundialmente como Verisign, por exemplo, com certificado da Claro ou do Parceiro garantindo sua integridade e originalidade.*
6. *Interação com outros usuários*
   a. *A interação com outros usuários dos serviços por site ou por celular, seja para troca de mensagens ou disponibilização de conteúdo on-line deve ser monitorado e permitir rastreamento e monitoramento em caso de Mandatos Judiciais e quebra de Sigilo;*
   b. *A geração de logs de todas as ações realizadas pelos usuários é critica e deverá atender ao padrão de geração de Logs;*
7. *Utilização de Serviços de SMTP/SMS*
   a. *A interação com outros usuários dos serviços por site ou por celular, seja para troca de mensagens ou disponibilização de conteúdo on-line deve ser monitorado e permitir rastreamento e monitoramento em caso de Mandatos Judiciais e quebra de Sigilo;*
   b. *A geração de logs de todas as ações realizadas pelos usuários é critica e deverá atender ao padrão de geração de Logs.*
8. *Utilização de Serviços de GSM (rastreamento)*
   a. *A interação com outros usuários dos serviços por site ou por celular, seja para troca de mensagens ou disponibilização de conteúdo on-line deve ser monitorado e permitir rastreamento e monitoramento em caso de Mandatos Judiciais e quebra de Sigilo;*
   b. *A geração de logs de todas as ações realizadas pelos usuários é critica e deverá atender ao padrão de geração de Logs.*
9. *Gerenciamento de Bônus e Benefícios*
   a. *Caso o cliente possa realizar ações que possam causar impactos aos produtos contratados pela interface Web e o serviço não esteja integrado ao Minha Claro/Senha Única sempre será necessário um 2º fator de autenticação que garanta que o cliente é ele mesmo para confirmar a aceitação do Bônus/Benefício.*
10. *Realização de Compra/Venda de produtos/serviços*
    a. *Formas de Pagamento*
       i. *A entrada de dados de pagamento como cartão de crédito devem ser tratados de forma sigilosa, tais dados não poderão ser armazenados localmente e seu tráfego deverá ser realizado de forma criptografada com a utilização de protocolo SSL.*

Passo 5 – Ativação/Cancelamento de Serviços

a. *Caso o cliente possa realizar ações que possam causar impactos aos produtos contratados pela interface internet e o serviço não esteja integrado ao Minha Claro e ao Senha Única sempre será necessário um 2º fator de autenticação que garanta que o cliente é ele mesmo para confirmar a aceitação da Ativação/Cancelamento;*
b. *A geração de logs de acessos e alterações/consultas realizadas pelos clientes é critico, portanto sua implementação é mandatória.*

Passo 6 – Geração de Relatórios

a. *O sistema deverá permitir ao usuário/cliente a geração de Relatório de utilização de serviços;*

Passo 7 – Gestão de Logs

1. *Geração*
   a. *O sistema deve gerar registros de auditoria (log) contendo as atividades executadas pelos usuários, exceções e outros eventos de segurança em todas as camadas da aplicação;*
   b. *Os registros de auditoria devem ser mantidos em um ambiente controlado que não permita alterações nem por parte dos administradores dos sistemas;*
   c. *Os logs das aplicações devem ser armazenados em Banco de Dados ou no formato de texto separado por delimitadores;*
   d. *Devem ser registrados em log todas as ações como: Leitura, execução, alteração, inclusão ou exclusão de dados ou configurações para qualquer perfil de usuário:*
      i. *ID do usuário*
      ii. *Data e hora da atividade*
      iii. *Identificação do terminal de origem; (Endereço IP)*
      iv. *Registro da atividade (Descrição resumida da regra de negócio envolvida, se possível organizada através de códigos);*
      v. *Dados acessados ou manipulados e tipo de acesso/manipulação.*

2. *Armazenamento*
   a. *O armazenamento mínimo de log de forma on-line é de 30 dias, os demais serão transferidos para backup por um período mínimo de 5 anos;*
   b. *O armazenamento deve ser realizado em mídias seguras que permitam seu restore em tempo hábil para realização de investigações solicitadas pela policia;*
   c. *Estes backups devem ser armazenados de forma segura protegido contra roubo ou destruição.*

3. *Expurgo*
   a. *A empresa deve apresentar a Claro seu processo de expurgo de logs após o prazo de 5 anos.*
   ATENÇÃO: *Caso o contrato seja extinto num prazo inferior à 5 anos, todo o log gerado ao longo do período deverá ser disponibilizado para a Claro em mídia e formato compatível com as tecnologias atuais.*

4. *Disponibilização/Consulta*
   a. *A empresa deverá respeitar o SLA estabelecido pela Claro para atender as requisições de investigação;*
   b. *A empresa deverá disponibilizar os logs solicitados pela Claro de forma restrita e segura, através de página Web autenticada ou transferência dos arquivos de Log. Este processo deverá ser definido em contrato entre a Claro e o Parceiro.*

Passo 8 – Interceptação

1. *Monitoramento do usuário*
   a. *O parceiro deverá ter ferramentas ou processos que permitam o monitoramento de determinados usuários em caso de solicitação judicial.*

2. *Quebra de Sigilo*

a. *O parceiro deverá ter ferramentas ou processos que permitam a quebra de sigilo de uma determinada conta de usuário/parceiros em caso de solicitação judicial.*

2. Segurança HotSite Atendimento

Passo 1 – Cadastro dos Usuários do Atendimento

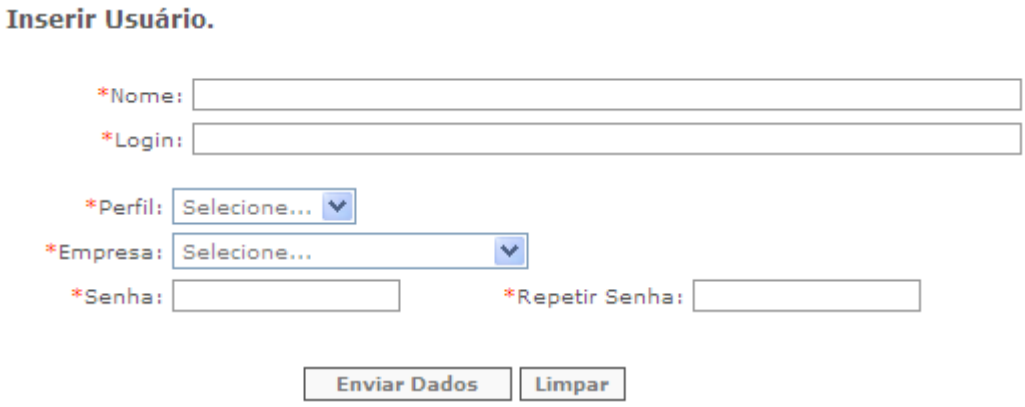
1. *Integração ao LDAP/AD Claro*
   a. *De preferência deve-se integrar a aplicação ao AD/LDAD da Claro;*

2. *Em caso de Não-Integração com o LDAP/AD Claro*
   a. *A empresa deverá disponibilizar uma ferramenta conforme as especificações de SIC abaixo para o sistema de Gerenciamento de Usuários:*

A CLARO reserva-se o direito de acrescentar/alterar os requisitos de Gerenciamento de Usuários sempre que necessário, mediante notificação formal ao fornecedor.
O Parceiro por sua vez deverá medir os esforços e definir um plano para implementação dos novos requisitos, respeitando sempre às expectativas e prazos reservados ao Projeto.

Tela padrão para criação de usuário

A interface de criação de usuários deverá ser composta basicamente dos seguintes campos:



IMPORTANTE: *Na consulta de um usuário a ferramenta deve fornecer além dos dados cadastrais, o status da conta. (Ex. Bloqueado por Senha Incorreta / Ativo / Bloqueado por Fraude).*

Funcionalidade para cadastramento de usuários em massa com base numa listagem pré-definida

Deve estar presente na ferramenta de Gerenciamento de Usuários uma funcionalidade que permita a criação de usuários em massa, à partir de arquivo texto com formato pré-definido (txt, csv, xls, separado por , ou ; ou colunas).

FORMATO ➔ Login, Nome Completo, Perfil, Empresa, Senha

Exemplo:

12345678, Paulo dos Santos, Consulta, TimWe, 123$ec!!

87654321, Carlos de Freitas, Administrador, Claro, 753@Adm#

O sistema deverá retornar a quantidade de:

- *Usuários cadastrados pela rotina atual;*
- *Usuários não cadastrados;*
- *Usuários que já existiam no sistema.*

Funcionalidade para exportar usuários em massa

A ferramenta deve possuir uma funcionalidade que permita ao Administrador do Sistema realizar um EXPORT de todos os usuários cadastrados na aplicação, no seguinte formato.

FORMATO ➔ Login, Nome Completo, Perfil, Empresa, Status

Exemplo:

12345678, Paulo dos Santos, Consulta, TimWe, Ativo

87654321, Carlos de Freitas, Administrador, Claro, Bloqueado

Funcionalidade para bloquear usuários em massa

*A ferramenta deve proporcionar o **bloqueio** em massa de usuários, à partir de um arquivo texto contendo o login do usuário e o motivo do bloqueio (os motivos não devem ser fixos).*

FORMATO ➔ Login, Motivo de Bloqueio

Exemplo:

12345678 – Bloqueio por Demissão

87654321 – Bloqueio Falta de Validação do Gerente

Funcionalidade para resetar usuários em massa

*A ferramenta deve prever o **reset da senha** em massa de usuários, à partir de um arquivo texto contendo o login do usuário e o nova senha (os motivos não devem ser fixos).*

FORMATO ➔ Login, Nova Senha

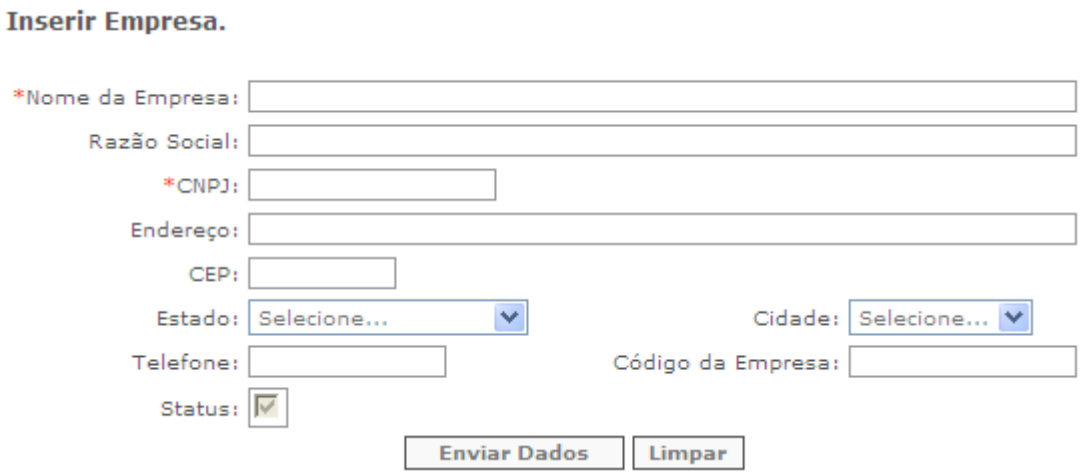
Exemplo:

12345678, 123$ec!!

87654321, 753@Adm#

Tela para cadastramento de Empresas (Parceiros da CLARO)

A ferramenta deve possuir uma tela que permita o cadastramento das empresas (prestadores de serviços) que trabalham com a CLARO, para diferenciar os usuários internos e os usuários externos por empresa. Basicamente a tela deve ser composta dos seguintes campos:



Política de Senha

A aplicação deve seguir a Política de Senha vigente na Claro, que define:

- ✓ *No mínimo 8 (oito) caracteres para a composição da senha (sendo números, letras e caracteres especiais);*
- ✓ *A senha inicial deve expirar no primeiro acesso (criação e reset da senha);*
- ✓ *A nova senha não poderá ser igual às últimas 12 (doze) senhas utilizadas;*
- ✓ *O período de expiração da senha deve ser de 30 (trinta) dias à partir da data de sua criação;*
- ✓ *Todo e qualquer acesso deve ser bloqueado após 5 (cinco) tentativas incorretas.*

Passo 2 – Acesso ao Site (Administração de Logins e do Atendimento)

1. *Autenticação*
   a. *Os usuários deverão entrar com login e senha;*

2. *Disponibilidade da aplicação*
   a. *A aplicação somente deverá estar disponível através de uma VPN ou para os IP's públicos registrados para a CLARO, de forma que não sejam permitidos acessos através da Internet;*

3. *Deverá possuir Certificado Digital (Https);*

4. *Não deverá permitir acessos simultâneos (apenas uma sessão por login).*

Passo 3 – Geração de Relatórios

1. *A aplicação deverá disponibilizar funcionalidades de geração de relatórios administrativos quanto ao gerenciamento dos logins realizados por esta interface.*

Passo 4 – Gestão de Logs

1. *Os registros de auditoria devem fornecer informações necessárias para sua utilização em futuras investigações, sendo que devem conter no mínimo;*
   a. *ID do usuário*
   b. *Data e hora da atividade;*
   c. *Identificação do terminal de origem (endereço IP);*
   d. *Registro da atividade (Descrição resumida da regra de negócio envolvida; cada tipo de atividade deverá ter um código de classificação "event ID");*
   e. *Dados acessados ou manipulados e tipo de acesso/manipulação.*

f. *Cada sessão deverá permitir no máximo 15 (quinze) minutos de inatividade.*
g. *Estes logs devem ser atendidos para todos os perfis de usuários em qualquer situação seja: inserção, alteração, consulta ou utilização dos recursos do sistema.*
***IMPORTANTE:** O armazenamento mínimo de log de forma on-line é de 30 (trinta) dias, os demais deverão ser transferidos para backup (mantidos por 5 (cinco) anos). Os logs deverão estar disponíveis para consulta através da ferramenta de gerenciamento de usuários apenas para o perfil do máster (administrador).*

Passo 5 – Documentação

1. *Disponibilização de Manuais e Formulários*
   a. *O Parceiro deverá disponibilizar documentação/manual referente a interface de Gerenciamento de usuários;*
   b. *A partir desta documentação será realizado o treinamento das equipes de SIC e Atendimento;*
   c. *A documentação deverá estar em Português Brasil;*

Passo 6 – Testes Funcionais

1. *Testes Funcionais da Interface de Gerenciamento de Usuários*
   a. *O Parceiro deverá disponibilizar para Claro, antes da data de entrada em produção URL e login de acesso para testes das funcionalidades solicitadas para interface de Gerenciamento de usuários;*

3. Padrão de Segurança para Desenvolvimento Web para todas as interfaces (Cliente, Administrações de Logins e Atendimento)

Passo 1 – Apresentação

1. *Informações Pertinentes*
   a. *Este parte do documento tem por objetivo apresentar boas práticas de desenvolvimento seguro para aplicações Web. Os controles aqui descritos foram baseados em padrões de mercado mundialmente aceitos e implementados, como por exemplo, OWASP TOP 10 e SANS TOP 25 Most Dangerous Programming Errors.*
   b. *A implementação dos controles aqui apresentados, não significa que a aplicação estará livre de vulnerabilidades como um todo, mas sim que em seu desenvolvimento foram levadas em consideração boas práticas de codificação segura, diminuindo a superfície exposta a ameaças.*

Passo 2 - Padrão

1. *Validação de Entrada de Dados*
   a. *Quando um software falha na validação apropriada de entrada de dados, um usuário mal-intencionado é capaz de manipular os dados inseridos de uma forma não esperada, fazendo com que a aplicação receba inserções de dados que podem ser prejudiciais para a aplicação.*
   b. *Existem diversas abordagens que podem ser utilizadas para a manipulação e tratamento de dados inseridos pelo usuário, cada uma das abordagens poderá ser utilizada em situações diferentes, porém existem casos em que uma combinação de abordagens será necessária.*
      i. ***Blacklist** – esta abordagem emprega uma "lista negra" contendo um conjunto de strings literais ou padrões, que são reconhecidamente utilizados em ataques. O mecanismo de validação bloqueia qualquer dado que tenha um equivalente na "lista negra" e permite qualquer dado diferente disto. Normalmente este tipo de abordagem é considerado a menos efetiva por duas grandes razões. Primeiro, uma vulnerabilidade em uma aplicação Web pode ser explorada utilizando uma grande variedade de maneiras diferentes, e uma "lista negra" pode omitir alguns dos padrões utilizados. Em segundo, as técnicas de exploração evoluem constantemente;*
      ii. ***Whitelist** – esta abordagem emprega uma "lista branca" contendo um conjunto de strings literais, ou um conjunto de critérios. O mecanismo de validação permite os dados que possuam equivalentes na "lista branca" e bloqueiam todos os outros dados. Em casos onde este tipo de abordagem é exeqüível, é considerado o mais efetivo no tratamento de*

inserções de scripts maliciosos. Entretanto, em alguns casos, onde a gama de possíveis dados a ser inserido no parâmetro é muito grande e constantemente mutável, pode ser inviável a adoção desta abordagem;

iii. ***Saneamento*** *- esta abordagem reconhece a necessidade de algumas vezes aceitar dados que não podem ser tomados como seguros. Ao invés de rejeitar estas entradas de dados, a aplicação realiza um saneamento de várias maneiras para evitar que estes dados tragam algum efeito adverso. Potencialmente, caracteres considerados maliciosos podem ser removidos, permanecendo apenas o que é considerado seguro, ou eles podem ser adequadamente codificados ou "encapsulados" antes que um processamento adicional seja realizado;*

c. *Além do emprego das abordagens acima citadas, é extremamente importante que durante o desenho e desenvolvimento da aplicação, os seguintes itens sejam levados em consideração:*

i. *Utilize sempre um framework de validação de entrada de dados, como Struts ou o OWASP ESAPI API;*

ii. *Conheça e entenda todos os pontos da aplicação onde dados não confiáveis podem ser inseridos (Parâmetros, Argumentos, Cookies, qualquer dado lido da rede, variáveis de ambiente, cabeçalhos de requisições e seus conteúdos, componentes de URL, e-mail, arquivos, bancos de dados ou qualquer outro sistema externo que forneça dados para a aplicação). Realize a validação de dados em qualquer ponto onde exista uma interface de sua aplicação com qualquer ponto externo;*

iii. *Assuma que todo e qualquer tipo de entrada de dados é malicioso. Utilize, sempre que possível, a estratégia de Whitelist, rejeite qualquer tipo de entrada que não atenda as especificações feitas na whitelist, ou utilize o saneamento para transformar os dados potencialmente "perigosos" em dados inofensivos;*

iv. *Para qualquer tipo de validação de segurança realizada no lado cliente, assegure-se de duplicar a validação do lado do servidor, uma vez que qualquer tipo de controle implementado do lado do cliente poderá ser facilmente "driblado";*

v. *Não confie apenas na abordagem de Blacklist para detecção de inserções maliciosas. Existem muitos meios de codificação de dados e é possível que algumas delas sejam esquecidas;*

vi. *Quando a aplicação combinar dados de diversas origens, certifique-se de realizar a validação destes dados, antes de realizar a combinação dos mesmos;*

vii. *Converter o tipo das entradas de dados para o tipo de dados esperado pela aplicação, como por exemplo, utilizar uma função de conversão de string em número. Após a conversão para o tipo de dado esperado, assegure-se de que a entrada de dados se encaixe no range de valores esperados;*

viii. *As entradas de dados devem ser decodificadas e padronizadas para a representação de dados aceita pela aplicação. Assegure-se de que a aplicação não realiza a decodificação de dados mais do que uma vez;*

2. *<u>Codificação de Saída de Dados</u>*

a. *Uma aplicação deve preparar mensagens estruturadas para a comunicação com outros componentes (outros sistemas, browser, banco de dados, outros módulos, etc). Caso a codificação destas mensagens seja mal feita, um usuário mal-intencionado pode inserir comandos não esperados na aplicação. Se a aplicação utilizar entradas fornecidas por um usuário mal-intencionado na construção das mensagens sem a codificação apropriada, então o usuário mal-intencionado poderá inserir caracteres especiais que podem ser interpretadas como informação de controle ou metadado por outros componentes.*

b. *Durante o desenho e desenvolvimento da aplicação, os seguintes itens devem ser levados em consideração:*

i. *Procure entender em qual contexto os dados da aplicação serão utilizados e os codifique de acordo com a necessidade. Isto se torna especialmente importante quando os dados serão transmitidos entre componentes diferentes, ou quando são geradas saídas que possuem diversos tipos de codificação. Examine todos os protocolos de*

comunicação e representação de dados requeridos para determinar a melhor estratégia de codificação;

ii. *Procure utilizar mecanismos automatizados para a separação entre dados e código, estes mecanismos facilitam a codificação e validação de saída para todos os pontos onde a saída é gerada;*

iii. *Quando possível, na troca de informações entre componentes distintos, assegure-se de que todos os componentes envolvidos na comunicação utilizam o mesmo tipo de codificação de caracteres. Especifique o tipo de codificação que deve estar presente em todas as interfaces da aplicação;*

3. *Interação com SGBD (Sistema de Gerenciamento de Banco de Dados)*

a. *Aplicações geram consultas SQL dinamicamente, baseando-se apenas, em dados inseridos por usuários. Caso a aplicação não se utilize de mecanismos que impeçam que os dados inseridos modifiquem a estrutura esperada de uma consulta SQL, um usuário mal-intencionado pode inserir na consulta SQL, comandos de DDL (Data Definiton Language) ou DML (Data Manipulation Language), que podem ser utilizados para alterar a lógica da consulta de forma a "driblar" os controles de segurança existentes e realizar modificações na estrutura da base de dados de back-end.*

b. *Durante o desenho e o desenvolvimento da aplicação, os seguintes itens devem ser levados em consideração:*

i. *Considere a utilização de camadas de persistência, como hibernate, que fornecem, naturalmente, camadas de validação contra SQL Injection;*

ii. *Processe consultas SQL utilizando Prepared Statement, Consultas Parametrizadas ou Stored Procedure. Estas funcionalidades devem aceitar parâmetros ou variáveis, e para os casos onde for utilizadas Consultas Parametrizadas ou Stored Procedure, combine a utilização de filtros de caracteres especiais e comandos DDL e DML para as entradas de usuários;*

iii. *Siga o principio de menor privilégio na definição e criação do usuário de banco de dados da aplicação, ou seja, tenha em mente que o usuário deverá possuir permissão para realizar apenas as operações necessárias pela aplicação;*

iv. *Considere a utilização de mecanismos do SGBD que realizem nativamente a filtragem dos dados inseridos por usuários, como por exemplo, a package DBMS_ASSERT (Oracle) ou a API mysql_real_escape_string( );*

4. *Interação com o Sistema Operacional*

a. *Aplicações Web por muitas vezes realizam a ponte entre um usuário externo e o sistema operacional onde a aplicação reside. Quando a aplicação invoca qualquer programa residente no sistema operacional e permite que requisições maliciosas alimentem a string que posteriormente será utilizada na construção do código, ou parte do código, que invocará o programa, a aplicação abre portas para a utilização do sistema operacional com o mesmo permissionamento do usuário de sistema operacional que interage com a aplicação.*

b. *Durante o desenho e o desenvolvimento da aplicação, os seguintes itens devem ser levados em consideração:*

i. *Sempre que possível utilize chamadas a library ao invés de utilizar processos internos para recriar a funcionalidade requerida;*

ii. *Prefira executar os códigos gerados para chamadas ao sistema operacional em ambiente de "Jail" ou qualquer outro tipo de "Sandbox" que utilize uma fronteira entre os processos executados e o sistema operacional, restringindo a gama de comandos que podem ser gerados pela aplicação;*

iii. *Procure manter, o mais longe possível de alterações externas, os dados que serão utilizados na execução de algum comando de sistema operacional;*

iv. *Avalie os argumentos repassados para aplicação pelo usuário e remova qualquer tipo de caractere especial. Caso algum tipo de caractere especial seja necessário para o*

correto funcionamento da aplicação, utilize uma validação baseada em Whitelist, bloqueando qualquer tipo de caractere especial que não seja esperado;

v. *Caso o programa a ser executado permita que argumentos sejam especificados em um arquivo de entradas de parâmetro ou através de entrada apenas de argumentos, utilize estes métodos ao invés de utilizar construção de linhas de comando;*

vi. *Onde for possível, identifique qualquer função que invoque uma Shell de comandos utilizando uma string e substitua por uma função que requisite apenas argumentos;*

vii. *Execute a aplicação que receberá os comandos através de entradas de usuário, no contexto de menor privilégio possível para o seu funcionamento, evitando que um usuário mal-intencionado obtenha acesso a funções privilegiadas do Sistema Operacional.*

5. *Transmissão Segura de Dados Sensíveis*
   a. *Se uma aplicação transmite informações sensíveis através da rede, como dados confidenciais ou credenciais de acesso, estas informações atravessam diferentes pontos da rede até atingirem o seu destino final. Usuários mal-intencionados podem interceptar esta comunicação durante o trajeto e ter acesso aos dados sensíveis, e, tentativas de proteção dos dados através de codificações como base64 ou URL não surtirão efeito uma vez que estes tipos de codificação são facilmente desfeitas e os dados transformados em texto puro novamente. Para evitar que a interceptação de dados seja feita com sucesso:*
      i. *Aplicações que trafegam dados sensíveis devem ser projetadas para utilização em conjunto com um protocolo de comunicação seguro, como por exemplo, SSL;*
      ii. *Aplicações que trafegam dados sensíveis devem utilizar SSL para comunicação com todos os seus pontos e não somente nos pontos onde a informação sensível é trafegada;*

6. *Validação de Ações de Usuários*
   a. *Por padrão uma aplicação web não consegue realizar validações se uma requisição "bem-formada", válida e consistente foi intencionalmente enviada pelo usuário que a submeteu.*
   b. *Quando uma aplicação web é desenhada para receber requisições de usuários sem um mecanismo que realiza validações sobre esta requisição e se esta foi intencionalmente enviada por um usuário, torna-se possível para um usuário mal-intencionado persuadir um usuário válido da aplicação a realizar requisições não intencionais ao servidor web, que serão tratadas pela aplicação web como requisições autênticas. Isto pode ser feito através de URL forjada, carregamento de imagens, XMLHttpRequest, etc, e pode resultar em vazamento de informação, alteração de dados e execução não intencional de código malicioso. Para minimizar a possibilidade de que uma requisição não intencional seja aceita e processada por uma aplicação, é recomendado que:*
      i. *Verifique-se que a aplicação não possui a vulnerabilidade de Cross-Site Script (Controles apresentados em Validação de Entrada de Dados e Codificação de Saída de Dados), recomenda-se que esta validação seja feita através de um mapeamento de todos os parametros definidos pelo usuário e verificando se todos estes pontos de entrada estão tratados adequadamente;*
      ii. *A aplicação permita a utilização do método GET apenas para solicitação de dados e jamais utilize este método para qualquer modificação de dados. Esta ação, além de proteger a aplicação contra ataques de Cross-Site Request Forgery (CSRF), deixa a aplicação em conformidade com a RFC 2616 (HTTP/1.1);*
      iii. *A cada vez que um formulário é gerado pela aplicação, um número pseudo-randômico é atrelado a este formulário, quando um usuário válido submeter dados para tal formulário, a aplicação deverá verificar se o numero pseudo-randômico existe e se é igual ao número previamente gerado pela aplicação;*
      iv. *Identifiquem-se operações sensíveis na aplicação e implemente uma checagem dupla para estas ações, como por exemplo, enviando um pop-up para o usuário, perguntando se esta ação é desejada;*

v. *A aplicação realize validação do campo referer do cabeçalho HTTP, para garantir que a solicitação do usuário vem de uma parte esperada da aplicação. Embora este tipo de verificação não seja 100% confiável, pode ser considerada como parte de um mecanismo de defesa em profundidade;*

7. *Tratamento Apropriado de Erros*
   a. *Através de mensagens de erro uma aplicação pode divulgar informações a respeito de seu ambiente, usuários e dados processados ou em processamento no momento do erro. Uma informação deste nível poderá ser muito útil por si só, por exemplo, uma senha de usuário, ou pode ser útil na elaboração de um ataque mais devastador. Se um ataque falhar, um usuário mal-intencionado poderá utilizar as informações, obtidas através de uma mensagem de erros, para realização de um ataque mais focado. Para evitar o vazamento de informações através de mensagens de erro, recomenda-se que:*
      i. *As mensagens de erro devem retornar o mínimo de informações possíveis ao usuário final da aplicação;*
      ii. *Caso os erros devam ser registrados com alguns detalhes, direcione os detalhes para um arquivo de logs com acesso restrito apenas aos administradores da aplicação, as entradas de erro nos arquivos de log não devem conter informações como a senha do usuário ao qual o log foi gerado;*
      iii. *O tratamento de exceções deve ser realizado internamente pela aplicação e os erros contendo informações sensíveis não devem ser mostrados ao usuário final;*
      iv. *A funcionalidade de debug não seja habilitada em ambiente produtivo;*

8. *Controle de Acesso Apropriado (Autenticação e Autorização)*
   a. *Quando as verificações de controle de acesso não são aplicadas de forma consistente, usuários podem acessar dados ou realizar ações as quais eles não teriam permissões originalmente. Para evitar o acesso não autorizado a aplicações recomenda-se que:*
      i. *A aplicação possua sessões corretamente delimitadas para acesso anônimo, normal, privilegiado e administrativo;*
      ii. *A superfície de ataque seja reduzida através do mapeamento entre papéis (perfis) e funcionalidades;*
      iii. *O controle de acesso esteja de acordo com as regras de negócio estipuladas para a aplicação;*
      iv. *O controle de acesso do lado servidor seja verificado, de forma a não permitir que páginas sejam acessadas aleatoriamente através de acesso via URL;*
      v. *As aplicações realizem a autenticação dos usuários contra a base de usuários oficial da empresa;*
      vi. *O controle de funcionalidades da aplicação (Perfis de usuário) seja controlado através da própria aplicação e que o controle de usuários existentes nestes perfis seja controlado através da base de usuários oficial da empresa;*

9. *Utilização de Algoritmos de Criptografia*
   a. *A utilização de um algoritmo criptográfico fraco ou com vulnerabilidades conhecidas é um risco desnecessário que pode resultar em vazamento de informações sensíveis. A utilização de um algoritmo não padrão é muito perigosa uma vez que um usuário mal-intencionado pode ser capaz de quebrar este algoritmo e comprometer qualquer dado que seja protegido pelo mesmo, atualmente existem diversas técnicas para o comprometimento de algoritmos de criptografia padrão e não padrão. Ao escolher um algoritmo de criptografia para uma aplicação recomenda-se que:*
      i. *Não seja utilizado um algoritmo de criptografia desenvolvido internamente;*
      ii. *O algoritmo utilizado seja padrão de mercado e certificado pelo NIST FIPS 140-2, que é o padrão mais aceito pelo mercado mundial;*
      iii. *O algoritmo utilizado seja forte e livre de vulnerabilidades conhecidas, como por exemplo, AES-256 para criptografia e SHA-512 para hash;*

iv. *A aplicação seja projetada tendo em mente a facilidade de substituição de um algoritmo de criptografia, quando o utilizado se tornar obsoleto;*
v. *As chaves criptográficas sejam protegidas da forma correta, incluindo controle de acesso aos arquivos e diretórios do sistema operacional onde se encontram as chaves;*

10. *Utilização e Proteção de Senhas*
    a. *Em sistemas de Front-End a utilização de informações de usuário e senha, para acesso em sistemas de Back-End, embarcadas no código (Hard-Coded) da aplicação de Front-End constitui uma vulnerabilidade muito simples de ser explorada, devido à facilidade de conversão de arquivos binários (compilados ou pré-compilados) em código fonte. Em casos de aplicações Web onde o acesso ao código-fonte pode ser feito por qualquer usuário o risco de vazamento das informações de usuário e senha, de conexão com o sistema de Back-End, é ainda maior. Para evitar problemas com usuário e senha de conexão com sistemas de Back-End recomenda-se que:*

        i. *Armazene as informações de usuário e senha em arquivos de configuração criptografados onde as chaves para decriptação do arquivo estejam em diretório protegido contra acessos indevidos;*
        ii. *Em casos onde não for possível a utilização de arquivos criptografados, as informações de usuário e senha deverão ser armazenadas em arquivo de configuração mantidos em um diretório, do sistema operacional, onde o acesso seja o mais restritivo possível;*
        iii. *Em casos onde for estritamente necessário que as informações de usuário e senha constem no código-fonte, seja implementado um controle de acesso e execução ao código onde, por exemplo, sua execução ou acesso seja possível apenas através da console do sistema operacional, impedindo o acesso e execução através da rede;*

Passo 3 – Requisitos Adicionais

a. *A aplicação não deverá permitir mais de uma conexão simultânea com o mesmo login;*
b. *Todos os módulos das aplicações deverão identificar unicamente a sessão de cada usuário;*
c. *Todos os módulos das aplicações deverão contar com controles que impeçam o roubo de sessões;*
d. *As informações de identificação de sessões devem expirar após uma utilização, devendo ser renovada a cada ação do usuário no sistema;*
e. *A aplicação deverá contar com tempo de expiração da sessão do usuário em caso de inatividade. O tempo deverá ser parametrizável;*
f. *A aplicação deve dispor de recursos que impossibilitem tentativas de ataques sobre falhas de código de desenvolvimento;*
g. *A aplicação deverá verificar valores/parâmetros de entrada no sistema, não permitindo a entrada de caracteres que possam explorar ataques de Injection em Banco de Dados inclusive interação via browser*
h. *A aplicação deverá controlar os dados de entrada, onde for campo numérico só poderá ser digitado número, campos com entrada de caracteres especiais como data (/) cep (-) documentos (. -) deverão ser pré-fixado e os caracteres deverão ser adicionados automaticamente pela aplicação e tratados de forma que impeça sua utilização indevida pelos usuários;*
i. *A aplicação deverá realizar o tratamento de erros, inclusive exceções, de forma a não divulgar informações de sua estrutura ou arquitetura, mas simples o suficiente para orientar o usuário;*
j. *A aplicação deverá tratar à entrada de dados inválidos e processos não finalizados por algum problema, como corrigir, suspender ou cancelar a operação sempre gravando em logs ou alertando o administrador;*
k. *Todos Bugs ou Vulnerabilidades identificadas nos testes de segurança da Claro que possam trazer riscos ao ambiente deverão ser corrigidos;*

4. Terceirização de Infra-Estrutura

Passo 1 – Segurança Patrimonial

1. *Infra-Estrutura Física Geral*
    a. *A empresa contratada deverá contar com uma recepção/portaria que garanta a identificação de funcionários e visitantes que precisarão ter acesso ao ambiente da CONTRATADA. Inclusive a entrada e saída de veículos;*
    b. *A empresa deverá contar com grades e portões que impeçam a entrada de pessoas não autorizadas em áreas consideradas críticas para o negócio;*
    c. *A empresa CONTRATADA deverá contar com sistemas de proteção e segurança como alarmes e botão de pânico;*
    d. *A empresa CONTRATADA deverá ter processo formal de controle das chaves de áreas críticas da empresa e controle de acesso a elas;*
    e. *Para facilitar a identificação das pessoas que circulam pela empresa recomenda-se o uso de Crachás de identificação em local visível;*
    f. *A CONTRATADA deverá dispor de monitoração em circuito interno/externo de TV e a armazenagem das imagens, por um período de 30 dias, para verificação em caso de eventos de quebra de segurança;*
    g. *Todas as salas da CONTRATADA, designadas para o atendimento da Claro devem contar com ar-condicionado;*
    h. *Todas as salas da CONTRATADA devem possuir mecanismos de prevenção e controle de incêndios.*

2. *Infra-Estrutura Física – Exclusiva Claro*
    a. *A CONTRATADA deverá dispor de uma sala segregada e exclusiva para o atendimento dos serviços contratados pela Claro;*
    b. *A CONTRATADA deverá dispor de sistema eletrônico de controle de acesso e identificação do usuário, na entrada da sala exclusiva da Claro, de maneira a permitir somente o acesso de pessoas autorizadas.*

3. *Infra-Estrutura Física – Datacenter*
    a. *O Datacenter deverá contar ar-condicionado e equipamentos de controles de temperatura;*
    b. *O DataCenter deverá possuir mecanismos de prevenção e controle de incêndios.*
    c. *As entradas e saídas do Datacenter deverão ter controle de acesso de forma a identificar os usuários e ter um livro de assinatura, contendo o nome, RG, data, horário e motivo de acesso físico;*
    d. *O Datacenter deverá contar com no-break que garantam o tempo necessário de energia para que os servidores/equipamentos sejam desligados com segurança;*
    e. *A CONTRATADA deverá dispor de monitoração em circuito interno/externo de TV e a armazenagem das imagens, por um período de 30 dias, para verificação em caso de eventos de quebra de segurança.*

Passo 2 – Segurança de Informações TI

4. *Infra-Estrutura de Rede*
    a. *O segmento de rede que atenderá aos serviços contratados pela CLARO deverá ser segregado dos demais segmentos da rede do PARCEIRO a fim de evitar acessos indevidos ou cópia/leitura de informações em trânsito. A segregação deverá ser realizada através da utilização de VLANs, switches gerenciáveis exclusivos e firewalls. Conforme desenho representado acima;*
    b. *Os switches deverão contar com Access Lists com liberação através de endereçamento IP e MacAddress das estações autorizadas para atender os serviços contratados pela Claro;*
    c. *Todas as portas dos switches que não estiverem sendo utilizadas deverão ser bloqueadas pela CONTRATADA lógica ou fisicamente com controle de acesso;*
    d. *A rede deverá ser cabeada e todos os pontos identificados;*

e. *A CONTRATADA não poderá utilizar rede wireless no segmento de rede da Claro e qualquer outro ponto que trafegue suas informações;*
f. *O range de Endereçamento IP criado para a Claro deverá ser restrito e com máscara reduzida comportando apenas a quantidade de máquinas disponibilizadas para os analistas que trabalharão para à Claro;*
g. *Todas as segmentações de redes diferentes que não façam parte da prestação de serviços para a Claro deverão ser segregadas através de Firewall, seja para redes corporativas, datacenters ou internet;*
h. *A CONTRATADA deve controlar a saída de internet dos usuários através de proxy com autenticação.*

5. *<u>Desktops – Estações de Trabalho</u>*
   a. *As estações disponibilizadas para atendimento dos serviços contratados pela Claro deverão ser desktops;*
   b. *Não será permitida a utilização de notebooks ou qualquer dispositivo móvel com função de computador, como Palms ou Celulares que possam ser carregados facilmente para fora do escritório;*
   c. *As estações disponibilizadas para atendimento da Claro deverão ter no mínimo Sistema Operacional Windows 2000 SP4 ou Windows XP SP3;*
   d. *Todas as estações disponibilizadas para a prestação de Serviços para a Claro deverá contar com Antivírus instalado, configurado e atualizado. Será necessária a geração de relatórios esporádicos a pedido da Claro;*
   e. *A CONTRATADA deve dispor de processo de Instalação, Configuração e Atualização de Patches de Segurança e de Correções de problemas de Hardware de Software para as estações e servidores disponibilizados para o Projeto com a Claro. Será necessária a geração de relatórios esporádicos a pedido da Claro;*
   f. *Todas as estações deverão ter seus leitores/gravadores de CD e DVD bloqueados, além das entradas USB e qualquer outro dispositivo que permita a cópia de dados, inclusive impressoras. A liberação destes itens deve ser controlada, justificada e sua utilização monitorada. Será necessária a geração de relatórios esporádicos de utilização a pedido da Claro;*
   g. *Todos os equipamentos disponibilizados pela CONTRATADA para prestação de Serviços a Claro não poderão dispor de modens;*
   h. *Todos os equipamentos disponibilizados pela CONTRATADA para prestação de Serviços a Claro deverão ser trancadas com cadeados impedindo a retirada de equipamentos que possam conter informações relevantes dos projetos da Claro;*
   i. *Todas as estações disponibilizadas para a realização do projeto da Claro deverão contar com a configuração do Limite de tempo de sessão (gerenciamento de bloqueio da estação após, no máximo, 10 minutos de inatividade);*
   j. *Todas as estações disponibilizadas para a prestação de Serviços para Claro deverão ter políticas de GPOs para controle de utilização de serviços, aplicativos e sistemas nas estações. Os aplicativos autorizados serão definidos após avaliação da criticidade do projeto em conjunto entre a Claro e a CONTRATADA;*
   k. *Todas as estações disponibilizadas para a prestação de serviços contratados pela Claro não deverão ser acessadas remotamente por seus funcionários, só poderão ser acessadas da localidade inspecionada pela CLARO.*

6. *<u>Datacenter – Infra-Estrutura e Servidores</u>*
   a. *Todo link internet que chegar a Rede da CONTRATADA deverá ter seu trafego tratado por firewall antes de chegar aos servidores e estações da rede corporativa;*
   b. *Qualquer periférico que permita a cópia de dados deve ter seu uso controlado e monitorado inclusive no processo de backup;*
   c. *A CONTRATADA deverá contar com ferramentas/equipamentos de backup;*
   d. *A CONTRATADA deverá contar com local seguro para gestão das fitas de backup;*
   e. *Os Servidores envolvidos no Atendimento do Contrato da Claro deverão estar com as últimas versões de Sistema Operacional e com todos os patches de atualização e segurança instalados;*
   f. *Os Servidores envolvidos no Atendimento do Contrato com a Claro deverá contar com Antivírus instalado, configurado e atualizado;*

g. *Os Servidores envolvidos no Atendimento do Contrato com a Claro deverão contar com sistema de controle de utilização de devices externos e dispositivos via USB. Toda utilização deverá ser registrada, monitorada e controlada;*
h. *Em caso de configuração de VPN, a empresa CONTRATADA deverá ter firewall que suporte as seguintes configurações:*

IKE (Phase I Proposal)	
Diffie-Hellman Group	DH-2
Encryption Algorithm	AES-256
Hashing Algorithm	SHA
Renegotiate IKE every (lifetime)	28800 Sec
IPSEC (Phase II Proposal)	
Encryption Algorithm	AES-256
Hashing Algorithm	SHA
Renegotiate IPSEC every (lifetime)	3600 Sec
PSE ENABLE?	YES - DH-2

i. *Em caso de suporte de terceiros ao Firewall a empresa deverá realizar controle dos acessos realizados por esta empresa como bloqueio de regras quando esta estiver dando suporte ou então a troca de senhas de usuários administrativos e que tenham acesso ao firewall e infra-estrutura da empresa.*

Passo 3 – Segurança da Informação Corporativa

7. *Controle de Acesso*
   a. *A empresa deverá contar com procedimentos para gerenciamento de contas de usuários e sistemas. Deverá ser apresentado a Claro um documento onde esteja descrito o processo realizado para solicitação de criação, exclusão e bloqueio de usuários;*
   b. *A empresa deverá contar com procedimentos para gerenciamento de contas de usuários Administrativos de domínio ou locais; Deverá ser apresentado a Claro um documento onde esteja descrito o processo realizado para solicitação de criação, exclusão e bloqueio destes usuários;*
   c. *Na demissão do funcionário ou na rescisão de contratos (sub-contratados), os identificadores individuais (contas) deverão ser removidos e os responsáveis comunicados;*
   d. *A empresa CONTRATADA não poderá utilizar contas genéricas em processos/usuários envolvidos na prestação de serviços a Claro;*
   e. *Todos os funcionários deverão dispor de login único e password pessoal e intransferível;*
   f. *Todas as senhas dos usuários deverão ser compostas por um mínimo de caracteres igual ou superior a 8, conter caracteres especiais, alfa-numérico, maiúsculas e minúsculas e expiração com tempo máximo de 30 dias;*
   g. *Todas as contas devem ser bloqueadas após 3 tentativas inválidas;*
   h. *A EMPRESA CONTRATADA deve Impedir que o usuário possua privilégios de administração em sua estação de trabalho, evitando-se assim que o mesmo possa instalar softwares e alterar configurações do sistema operacional ou de aplicações instaladas. No caso de necessidade de acessos privilegiados deverão ser criados com permissões exclusivas para execução do processo necessário e não permissão full administrativa;*
   i. *Os funcionários da CONTRATADA não deverão utilizar-se de Webmails e áreas de armazenamento de dados públicos, como forma de se evitar a evasão de informações da CLARO. Qualquer site a ser utilizado pela equipe envolvida no projeto da Claro deverá ser justificado e autorizado pelo Gerente do projeto na CONTRATADA. Deverá ser apresentado a Claro o processo para solicitação e justificava da liberação de sites para os analistas.*

8. *Custódia de Informações*
   a. *Todos os acessos, alterações, inclusões, erros, sucessos ou qualquer outra execução realizada pelos usuários nos sistemas da CONTRATADA que tiverem ligação com a Prestação de Serviços a Claro deverão ser registradas em logs por um período mínimo de 3 meses on-line e 5 anos (ou por até 6 meses após o final do contrato com Claro) armazenados através de backup;*
   b. *A CONTRATADA não deve de forma voluntária inserir no código fonte das aplicações desenvolvidas por ela, funcionalidades ou códigos que permitam a quebra de segurança da aplicação;*

c. *Em caso de Incidentes de Segurança a CONTRATADA deverá informar imediatamente a CLARO, para que sejam tomadas as providências cabíveis mediante a gravidade do incidente;*
d. *A CONTRATADA deverá contar com Plano de Continuidade de Negócios e documentação de referencia, garantindo a contingência e recuperação em caso de incidentes. Estes devem ser adequados ao Acordo de Nível de Serviços celebrado com à Claro;*
e. *A CONTRATADA deverá dispor de processos de rotinas de backup e do descarte de fitas ou outros dispositivos que armazenem algum tipo de informação disponibilizada pela CLARO para a realização do projeto ou prestação de serviços; Deverá ser disponibilizado para a Claro um documento com a descrição do processo que será realizado;*
f. *A CONTRATADA deverá contar com processos de Criptografia de Dados considerados como Confidenciais pela Claro, seja para armazenamento em Banco de Dados ou diretórios de arquivos ou transferência de informações (Client x Server);*
g. *A CONTRATADA deverá dispor de local seguro para armazenamento de documentos impressos referente à prestação de serviços a Claro;*
h. *Os processos e mecanismos adotados para a transmissão de qualquer informação devem fornecer segurança quanto à autenticidade, confidencialidade e integridade da informação e são definidos pela Claro;*
i. *A CONTRATADA deverá contar com rotinas de backup diárias seja full ou incremental de forma que seja possível restaurar a última posição integra antes de um possível incidente;*
j. *A CONTRATADA não deverá em hipótese alguma realizar cópias das informações disponibilizadas pela CLARO sem autorização formal;*
k. *As informações pertencentes a CLARO e/ou geradas pela EMPRESA CONTRATADA necessárias para a realização da atividade contratada devem ter o acesso restrito às pessoas autorizadas;*
l. *A CLARO reserva-se o direito de realizar avaliações de risco de segurança quer seja através de sua equipe de Auditoria de sistemas ou através de empresa por ela contratada. Estas avaliações deverão ser agendadas com antecedência e acompanhadas pela área de segurança da EMPRESA CONTRATADA, e durante estas visitas documentações e informações pertinentes aos sistemas e ambiente computacional poderão ser solicitadas a EMPRESA CONTRATADA.*

5. Processo de Testes de Segurança das Aplicações

Passo 1 – Analise Funcional

1. *Testes dos Requisitos de Segurança Solicitados*
   a. *Nesta fase de testes é avaliado o nível de implementação dos requisitos funcionais e de negócio solicitados pelas equipes de Segurança. Qualquer pendência é reportada para equipe técnica (interna ou externa) da falta de implementação do requisito e sua criticidade;*

2. *Tempo de Cronograma para realização dos Testes Funcionais*
   a. *1 Semana*

Passo 2 – Analise Automatizada/Manual

1. *Testes dos Requisitos de Segurança para desenvolvimento*
   a. *Fase 1 – Teste Automatizado*
      i. *A Claro utiliza ferramentas de mercado para execução de testes que tentam explorar vulnerabilidades nas aplicações ou seu código. As ferramentas são compostas por Bases de Vulnerabilidades, onde estão catalogadas vulnerabilidades por linguagem de desenvolvimento, sistema operacional, banco de dados etc;*
   b. *Fase 2 – Teste Manual*
      i. *Após a realização dos testes automatizados todas as vulnerabilidades encontradas são testadas de forma manual, de forma a garantir que não hajam "falsos-positivos" e que otimize assim as correções pelo parceiro.*

2. *Tempo de Cronograma para realização dos Testes Automatizado/Manual*
   a. *1 Semana*

Passo 3 – Geração de Relatório

1. *Relatório de Analise Funcional*
    a. *Ao final desta fase é gerado um relatório para a área responsável pelo projeto com o status de implementação dos requisitos implementados e as também o que está pendente além da descrição da criticidade de cada item;*

2. *Relatório de Analise Automatizada/Manual*
    a. *Ao final desta fase é gerado um relatório para a área responsável pelo projeto com o status de implementação dos requisitos implementados e as também o que está pendente além da descrição da criticidade de cada item;*

3. *Tempo de Cronograma para Geração de Relatório*
    a. *1 Semana*

Passo 4 – Teste Final

1. *Relatório Final*
    a. *Após as correções pelo parceiro a Claro realiza novamente os testes Funcionais, Automatizados e Manuais e valida a implementação das correções. Ao final do relatório é passada a Conclusão Final de autorização ou não para a entrada em produção da aplicação.*

2. *Tempo de Cronograma para realização dos Testes Finais + Geração de Relatório Final*
    a. *1 Semana*

6. Observações Adicionais

Passo 1 – Emissão do Termo de Confidencialidade

1. *Empresa*
    a. *Ao iniciar os primeiros contatos comerciais com a empresa a ser contratada é necessária a assinatura do Termo de Confidencialidade com a Claro;*
        i. *Este deverá ser emitido pela Juridico da Claro e armazenado por ele;*

2. *Funcionários*
    a. *Em caso de projetos de alto risco além do termo de confidencialidade assinado pela empresa é necessário que os funcionários/terceiros envolvidos com o projeto também tenham Termo de Confidencialidade assinado com a empresa contratada;*

3. *Empresas "Quarterizadas"*
    a. *Em caso de terceirização de serviços pelo parceiro com outras empresas estas também devem ter o termo de confidencialidade assinado com a empresa contratante;*

Passo 2 – Termo de Responsabilidade

1. *Empresa*
    a. *A empresa contratada deverá ter conhecimento das responsabilidades que ela terá com a prestação de serviços a Claro e ter noção de sua co-responsabilidade quanto a danos que possam ser ocasionados a terceiros, caso não sejam implementados os requisitos de Segurança solicitados e básicos de mercado;*

2. *Empresas "Quarterizadas"*
    a. *A empresa terceirizada pela contratada deverá ter conhecimento das responsabilidades que ela terá com a prestação de serviços e ter noção de sua co-responsabilidade quanto a danos que possam ser*

ocasionados a terceiros, caso não sejam implementados os requisitos de Segurança solicitados e básicos de mercado;

Passo 3 – Contratos de Prestação de Serviços

1. *Empresa*
   a. *Deverão estar previstos em contrato as responsabilidades da empresa quanto a:*
      i. *Danos de Imagem a Claro e a seus clientes;*
      ii. *Vazamento de Informações;*
      iii. *Monitoramento e Quebra de Sigilo;*
      iv. *Quebra de Integridade e Confidencialidade dos dados;*
      v. *Transferência de Domínios de Internet;*
      vi. *Co-responsabilidade referente ao gerenciamento de certificados digitais emitidos pela Claro;*
      vii. *Outros que sejam definidos com o perfil do projeto a ser desenvolvido.*