REQUISITO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

CONTRATAÇÃO DE SERVIÇOS DE TERCEIROS DE DESENVOLVIMENTO SEGURO DE SISTEMAS

CONTROLE DE VERSÃO

DATA	*VERSÃO*	*RESPONSÁVEL*
11.09.2020	*00*	*Nilson Luiz Tedeschi / Paulo Quito*
28/07/2021	*01*	*Nilson Luiz Tedeschi / Paulo Quito*
07/03/2022	*02*	*Nilson Luiz Tedeschi / Paulo Quito*

** Este documento está alinhado à NR-SEG-004*

SUMÁRIO

1. OBJETIVO

Apresentar os requisitos de Segurança da Informação e Privacidade obrigatórios que deverão ser observados pela CONTRATADA, relativos aos padrões e premissas arquitetônicas para o desenvolvimento e manutenção dos sistemas, aplicações e aplicativos de forma a uniformizar e garantir seu modo de funcionamento e aplicação, considerando o processamento, transmissão e/ou armazenamento de informações de clientes e colaboradores da CLARO.

2. APLICAÇÃO

Aplica-se à Claro S.A. e suas Controladas/Coligadas, bem como para todos aqueles que, mesmo não sendo colaboradores próprios, trabalhem dentro ou fora das instalações das Empresas ou ainda que tenham acesso às informações dos processos da Organização.

3. REFERÊNCIAS

Os seguintes documentos referenciados, no todo ou em parte, são normativas e padrões de mercado:

Para o desenvolvimento deste documento, foram considerados:

- **ABNT NBR ISO/IEC 27001:2013:** Tecnologia da Informação — Técnicas de Segurança — Sistemas de Gestão da Segurança da Informação;
- **ABNT NBR ISO/IEC 27002:2013:** Tecnologia da Informação — Técnicas de Segurança — Código de Prática para Controles de Segurança da Informação;
- **ABNT NBR ISO/IEC 27005:2011:** Tecnologia da Informação — Técnicas de Segurança — Gestão de Riscos de Segurança da Informação;
- **ABNT NBR ISO/IEC 27011:2008:** Técnicas de Segurança - Diretrizes para Gestão da Segurança da Informação para Organizações de Telecomunicações.
- **ABNT NBR ISO/IEC 27017:2016** - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação com Base ABNT NBR ISO/IEC 27002 para Serviços em Nuvem;
- **ABNT NBR ISO/IEC 27701:2019:** Tecnologia da Informação — Técnicas de Segurança — Extensão à ABNT NBR ISO/IEC 27002 para Gestão da Privacidade da Informação – Requisitos e Diretrizes;
- **CÓDIGO DE ÉTICA**, do Grupo América Móvil;
- **DECRETO Nº 8.771/2016** – Decreto que regulamenta o Marco Civil da Internet;
- **LEI Nº 12.965/2014** – Marco Civil da Internet;
- **LEI Nº 9.472/97:** Lei Geral das Telecomunicações;
- **LEI Nº 13.709/18** - Lei Geral de Proteção de Dados Pessoais;
- **LEI Nº 13.853/19** – Lei que altera a LGPD e cria a Autoridade Nacional de Proteção de Dados;
- **Normas de Segurança da Claro.**
- **NIST SPECIAL PUBLICATION 800-64 Revision 2** - Security Considerations in the System Development Life Cycle;
- **OWASP SECURE CODING PRACTICES 2.0** - Guia de Referência Rápida de Práticas de Codificação Segura;
- **PCI-DSS 3.2.1 (PAYMENT CARD INDUSTRY** – DATA SECURITY STANDARDS) - Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS).

.

4. REQUISITOS DE SEGURANÇA PARA CONTRATAÇÃO DE SERVIÇOS DE TERCEIROS

4.1. Organização de Segurança da Informação e Proteção de Dados Pessoais

i. Para fins de organização da Segurança da Informação e da privacidade e proteção de dados pessoais, a CONTRATADA deve:

a) Possuir um modelo de gestão de Segurança da Informação e Privacidade, com o papel de elaborar, divulgar e atualizar as políticas e diretrizes de segurança e proteção de dados pessoais, que deverão ser apresentadas à Claro em caso de solicitação nesse sentido;

b) Designar um responsável pelo modelo de gestão de Segurança da Informação, que deverá atuar na gestão e no cumprimento das diretrizes e, se aplicável, um DPO, responsável pela estrutura e governança do programa de privacidade e proteção de dados pessoais;

c) Possuir uma política de Segurança da Informação (ou documento similar) revisada periodicamente e divulgada a todos os funcionários e terceiros, em que conste diretrizes de segurança e privacidade, contendo, no mínimo, os seguintes temas (não se limitando somente a estes):

- Classificação da Informação, inclusive de Dados Pessoais
- Mesa e tela limpa
- Segurança física
- Controle de acesso
- Senhas
- Manuseio da informação
- Licenciamento de software
- Backups
- Resposta a incidentes de segurança e de privacidade
- Acesso à internet
- Uso de correio eletrônico
- Procedimentos documentados
- Gestão de vulnerabilidades / patches
- Governança em privacidade
- Registro de tratamento de dados pessoais

d) Documentar e manter atualizados os processos e procedimentos internos relacionados à prestação do serviço e aos requisitos de Segurança da Informação e Privacidade (ISO 27701:2019);

e) Realizar durante a contratação e periodicamente treinamentos de conscientização para seus funcionários sobre os aspectos de Segurança da Informação e Privacidade exigidos neste documento;

f) Cumprir a legislação e regulamentações aplicáveis à prestação de serviço, particularmente a Lei Geral das Telecomunicações e a LGPD;

g) Designar responsáveis, custodiantes e usuários das informações de seus sistemas internos.

ii. Caso o serviço prestado envolva transações de cartões de pagamento, a CONTRATADA deverá estar em conformidade com o padrão PCI-DSS, evidenciando anualmente sua conformidade de acordo com as regras do PCI, bandeiras e adquirentes;

iii. Todas as informações de propriedade da Claro, bem como as de seus clientes devem ter sua utilização restrita à prestação do serviço contratado e devem ser tratadas como confidenciais, sendo assegurado o acesso dos profissionais às informações apenas na medida necessária à execução de suas tarefas.

4.1.1. Proteção de Dados Pessoais e Dados Pessoais Sensíveis

i. Os controles de segurança de informações e TI devem ser aplicados para garantir que os dados sejam protegidos adequadamente nos termos da ABNT NBR ISO/IEC 27701:2019;

ii. A CONTRATADA, além de assumir a responsabilidade de garantir que a transferência eletrônica de dados pessoais entre ele e outros terceiros seja devidamente protegida, deve solicitar formalmente aprovação à Claro para efetuar o compartilhamento dos dados;

iii. Deve também impedir o acesso direto aos dados confidenciais do processo em que são armazenados e processados;

iv. O acesso do usuário a dados confidenciais só deverá ser possível quando for absolutamente necessário. Todo o acesso deve ser auditável para identificar a data, hora, atividade e pessoa responsável;

v. Administradores de sistema e banco de dados podem ter acesso privilegiado a dados confidenciais, porém este deve ser autorizado e monitorado;

vi. O acesso administrativo aos dados somente ocorrerá quando explicitamente autorizado e sempre será irreversivelmente registrado;

vii. Os dados devem ser armazenados e protegidos de acordo com sua classificação;

viii. Todas as informações, dados pessoais e dados pessoais sensíveis de clientes da Claro devem ser criptografadas;

ix. Conforme normas de Segurança da Informação da Claro, a transmissão deve:

a) Ser criptografada para manter a confidencialidade e a integridade das informações;

b) Ser controlada, em conformidade com a legislação pertinente;

c) Estar protegida contra interceptação, cópia, modificação, desvio e destruição;

d) Contemplar o uso de um protocolo seguro para comunicação entre as partes com garantia de comunicação fim-a-fim.

x. Os controles de dados confidenciais devem estar sujeitos a um rigoroso programa de monitoramento interno, auditoria e manutenção para garantir a continuidade de sua operação correta;

4.2. Incidentes de Segurança e Privacidade

i. A estrutura de gerenciamento de Segurança da Informação da CONTRATADA deve manter e controlar a segurança por meio de uma equipe multifuncional que coordena a identificação, o agrupamento e a resolução de problemas de segurança, independentemente da estrutura do negócio;

ii. Deve ser mantido um mecanismo de resposta a incidentes, de segurança e privacidade, que inclua um processo para a investigação e mitigação de:

a) Violação acidental ou deliberada de regulamentos e procedimentos internos;

b) Suspeita ou detecção de comprometimento de sistemas ou recebimento de notificação de vulnerabilidades do sistema;

c) Invasão física ou lógica dos ativos ou informações;

d) Ataques de negação de serviço em componentes.

iii. No caso de incidente, a CONTRATADA deve:

a) Notificar imediatamente a Claro, através do e-mail csirt@claro.com.br, sobre a ocorrência de incidentes, irregularidades ou eventos suspeitos que afetem ou possam afetar a segurança das informações de propriedade da Claro;

b) Notificar imediatamente o responsável da Claro pela contratação;

c) Acionar o mecanismo de resposta a incidentes, a fim de mitigar os riscos

d) Garantir que os logs para análise ou perícia estejam disponíveis quando solicitados pela Claro.

4.3. Desenvolvimento

i. A CONTRATADA deve garantir as premissas básicas de Segurança da Informação e de Privacidade (finalidade, necessidade, confidencialidade, integridade, disponibilidade e autenticidade), bem como implementar processo de Privacy by Design, ambos previstos na ABNT NBR ISO/IEC 27701:2019, para todos os sistemas e/ou aplicações próprias, cumprindo, desta forma, o contrato firmado com a Claro que envolva manipulação de dados ou informações da Claro, inclusive dados pessoais de seus clientes;

ii. A CONTRATADA deve cumprir todas diretrizes e controles descritos no Anexo I ("Orientações de Desenvolvimento Seguro de Sistemas").

4.4. Utilização de E-mail

i. Toda comunicação com o cliente da Claro utilizando correio eletrônico deve ser feita utilizando os domínios corporativos definidos pela Claro e criptografia. A Claro não autoriza comunicação através de domínios públicos (ex: Gmail etc.);

ii. Todo e-mail com endereço corporativo da Claro disponibilizado a CONTRATADA deve ser configurado de acordo com os padrões de identificação e segurança vigentes e homologados pela Claro.

4.5. Gestão de Acessos

4.5.1. Autenticação

i. Os colaboradores da CONTRATADA devem utilizar uma credencial de acesso que será disponibilizada pela Claro, de modo a poder reconhecer (identificação) e comprovar (autenticação) a identidade do usuário no acesso aos sistemas de informação, recursos, áreas de processamento de dados e redes de comunicações que suportam a operação da CONTRATADA;

ii. Cada colaborador que necessitar de acesso para cumprimento do objeto do contrato com a Claro terá sua própria credencial de acesso, não sendo permitido seu compartilhamento ou utilização de usuários genéricos. Do mesmo modo, toda credencial de acesso terá um proprietário que será responsável pelas ações que sejam feitas;

iii. As senhas dos colaboradores devem ser de uso pessoal e intransferível; sendo:

a) Desabilitada a funcionalidade de lembrar a senha (*autocomplete*) nos campos de senha do navegador;

b) Adicionado controle de Captcha (*Completely Automated Public Turing test to tell Computers and Humans Apart)* em páginas onde houver entradas de usuário/senhas para evitar possíveis ataques de força bruta com dicionários à autenticação;

iv. Todas as credenciais dos usuários que tenham sido demitidos ou que tenham os serviços descontinuados devem ser desabilitadas e mantidas por um período (parametrizável), em atenção à base legal do tratamento dos dados pessoais relativos às credenciais de acesso, para que não seja perdido o histórico ou logs da mesma, em atenção à finalidade deste tratamento de dados pessoais e cumprimento às obrigações legais aplicáveis. As credenciais não poderão ser reutilizadas posteriormente;

v. No momento do desligamento de um colaborador da CONTRATADA envolvido na operação do serviço prestado para a Claro, a CONTRATADA deve imediatamente providenciar o cancelamento de todos os acessos. No caso de sistemas gerenciados pela CONTRATADA, os acessos devem ser removidos imediatamente por esta.

4.5.2. Autorização

i. Todo usuário que necessitar obter uma credencial de acesso em qualquer sistema deve passar por um processo de autorização. O processo deve contemplar e formalizar todas as etapas de solicitação, aprovação, execução, entrega e troca de senha;

ii. Todas as solicitações de liberação de acesso a informações, sistemas e/ou recursos devem ser obedecer aos critérios da Claro;

iii. Os perfis dos usuários devem ser definidos de acordo com a necessidade de uso e alinhados aos requisitos de negócios, considerando a imprescindibilidade ou não do acesso a dados pessoais;

iv. A CONTRATADA deve estabelecer um processo seguro para a entrega de senha;

v. Os sistemas e/ou aplicações utilizados na prestação de serviço contratado devem prever sua utilização por usuários com credenciais de acesso que possuam o mínimo privilégio necessário para exercer sua função, não devendo haver a necessidade de aumento dos privilégios destes usuários para a execução delas.

4.6. Registro de Auditoria e Arquivos de Log

i. A CONTRATADA deve:

a) Gerar e fornecer para a Claro registros que identifiquem todas as ações realizadas pelos colaboradores da CONTRATADA de forma que seja possível identificar qual foi o operador que executou cada ação executada, o momento de execução (data/hora), a duração, a partir de qual equipamento foi executado e quais dados pessoais foram objeto de tratamento (i.e., acessados, visualizados, compartilhados, etc.);

b) O processo de tratamento de dados pessoais e/ou o acesso a outras informações confidenciais pela CONTRATADA deve ser controlado a partir dos arquivos de log descritos nas alíneas “i” e “ii”, sendo possível obter um registro completo e a responsabilidade individual pelo ciclo de vida dos ativos de informação, de modo a garantir que todos os ativos criados, processados e excluídos são totalmente contabilizados.

ii. Os arquivos de log descritos no item acima devem ser armazenados de forma segura, possuindo restrição de acesso, principalmente nos casos de permissão de alteração e exclusão, e inviolável, mediante encriptação ou medidas de proteção equivalentes. O acesso e a leitura dos arquivos de logs devem ser restritos aos usuários autorizados;

iii. Não deve existir nenhum processo ou função que altere ou apague qualquer registro dos arquivos de log e, portanto, da trilha de auditoria, salvo o script de retenção;

iv. Os administradores de sistemas não devem ter permissão de exclusão ou desativação dos arquivos de log;

v. Deve ser realizado o sincronismo de relógio do ambiente a fim de assegurar a exatidão dos horários de ocorrência e credibilidade dos eventos registrados nos arquivos de log;

vi. Dados confidenciais utilizados na autenticação das credenciais de acesso (senhas, chaves privadas etc.) ou na autorização dos acessos (identificações ou senhas de sessão etc.) não devem ser registrados nos arquivos de log;

vii. Os ativos da CONTRATADA suportam o objeto do contrato devem prover no mínimo, mas não se limitando a:

a) Login do usuário;
b) Data;
c) Hora;
d) Tipo do evento;
e) Endereço do IP e Hostname do equipamento.

4.7. Tempo de Armazenamento

i. Os arquivos de logs de sistemas, recursos e redes que tramitem informações objetos do contrato firmado com a Claro devem ser armazenados on-line pelo **período mínimo de 6 (seis) meses;**

i. A CONTRATADA deve realizar as gravações das ligações de todas as operações realizadas para a Claro. As gravações devem ser armazenadas em locais seguros de acesso restrito por um período de, **no mínimo, 5 (cinco) anos;**

ii. Durante o cumprimento do contrato, o prazo de armazenamento poderá ser revisto pela própria Claro. A CONTRATADA deve estar ciente e preparada para se adequar em caso de alteração legislativa ou regulamentação pelas autoridades competentes, independentemente de prévia notificação da Claro de tal responsabilidade;

iii. A CONTRATADA deve definir um processo e um responsável para a disponibilização das gravações telefônicas à Claro. A Claro poderá solicitar a qualquer momento acesso a uma gravação e a CONTRATADA deve viabilizar sua entrega.

4.8. Descarte

i. As informações obtidas nos termos do contrato firmado com a Claro que forem armazenadas, processadas, transmitidas e tratadas devem ser destruídas ou devolvidas após término de contrato com a CONTRATADA ou quando solicitado por parte da Claro;

ii. As mídias digitais, tanto as fixas como as removíveis, que contenham dados e informações da Claro, quando não forem mais utilizadas, requerem os seguintes cuidados no descarte:

a) Identificar e registrar as mídias que requerem descarte seguro, tais como fitas de backup, discos rígidos, DVDs, impressos e outros;

b) Triturar, incinerar ou inutilizar as mídias para que os dados não possam ser recuperados;

c) Os serviços terceirizados de coleta e descarte de papel, de equipamentos e de mídias magnéticas, deve ser efetuado por fornecedor com experiência e controles de segurança adequados.

4.9. Gestão de Vulnerabilidade

i. A CONTRATADA deve manter um banco de dados ou ferramenta de inventário atualizada sobre ativos tecnológicos, sistemas operacionais e softwares base instalados na CONTRATADA, que inclua as informações de fabricantes, versões, níveis de atualização de patches e, no caso de software base, o sistema operacional em que este se encontra instalado;

ii. Implementar as correções de segurança (patches), conforme disponibilizadas pelos respectivos fabricantes dos softwares que suportam as operações;

iii. A CONTRATADA deve entregar para a Gerência de Segurança da Informação Corporativa da Claro, a cada 3 (três) meses, um relatório com plano de tratamento das vulnerabilidades identificadas. O resultado do trabalho não pode conter vulnerabilidades críticas;

iv. A CONTRATADA deve definir um procedimento para calcular o risco de cada vulnerabilidade identificado, considerando critérios de classificação da informação, probabilidade de exploração da vulnerabilidade e o impacto relacionado.

4.10. Gestão de Continuidade de Negócios

i. A CONTRATADA deve assegurar a disponibilidade de seus ambientes, conforme contratado, considerando o tipo de atividade a ser exercida, sendo:

   a) Caberá a CONTRATADA fornecer, quando solicitado pela Claro (a qualquer momento), as informações referentes à infraestrutura que suporta as atividades, bem como o mapeamento das localidades e o número de estações de atendimento e/ou operação disponíveis em cada uma das localidades onde estas são prestadas;

   b) Caberá a Claro fornecer uma avaliação quanto aos negócios elegíveis e prioridade de recuperação das atividades.

ii. A CONTRATADA deve informar à Claro toda e qualquer alteração de infraestrutura e/ou recursos em seu ambiente de trabalho e nos ambientes de contingência que atuarem ou fizerem qualquer referência ao objeto ora contratado para o perfeito cumprimento desta cláusula;

iii. A CONTRATADA deverá implementar o Sistema de Gestão de Continuidade Negócio:

- Plano de Gestão de Crise (exemplo: crise hídrica e elétrica);
- Plano de Gestão de Incidente;
- Plano de Recuperação de Desastre;
- Plano de Contingência Operacional;
- Plano de Teste e Validação; e
- Plano de Comunicação.

iv. Deverá ser definido e documentado entre o gestor do contrato da Claro e a CONTRATADA o prazo e/ou tempo máximo e mínimo para recuperação dos dados e/ou serviços em caso de desastres;

v. Será necessário definir procedimentos e ações para a transferência das atividades essenciais do negócio para localidades alternativas até a resolução e avaliação do incidente;

vi. Os ativos críticos para a continuidade dos processos de negócios essenciais devem ser objeto de proteção redobrada e hospedados em local que permita o seu uso nos procedimentos de emergência mesmo em casos de desastres;

vii. Deve ser incluída capacitação e orientação de todos os envolvidos nos planos de continuidade de processos, estando aptos a desenvolver suas atribuições;

viii. Deverão ser realizados testes periodicamente dos planos e elementos de contingência, com coletas de evidências;

ix. A CONTRATADA deve garantir os backups das informações em consonância com as disposições legais, realizar periodicamente testes de restauração, bem como possuir infraestrutura de contingência: geradores, nobreak, redundância de servidores de hospedagem da página web, redundância de links, redundância de equipamentos críticos para operação, refrigeração, reservatórios de água, site alternativo, etc.;

x. Os recursos humanos da CONTRATADA, envolvidos nos Planos de Continuidade de Negócio (PCN), deverão ser treinados no tema, conforme as suas atribuições e responsabilidades nos planos;

xi. Devem ser identificadas as soluções táticas para suportar a restauração das atividades exigidas dentro de um tempo de recuperação desejado. Em cada caso, devem ser avaliadas as alternativas a fim de minimizar a probabilidade de um mesmo incidente afetar a solução de continuidade do negócio;

xii. Todo e qualquer incidente que comprometa a continuidade dos serviços deve ser comunicado de imediato ao gestor do contrato responsável, para as providências necessárias e, se necessário, acionar os respectivos planos de continuidade;

xiii. Devem ser desenvolvidos e implantados procedimentos para resposta e estabilização da situação após um incidente, utilizando-se dos planos de respostas específicos para cada tipo de cenário avaliado após a realização da análise de risco.

4.11. Segurança Lógica do Ambiente

i. Para as operações instaladas em ambientes/sites, a CONTRATADA deve:

a) Prover um segmento de rede exclusivo e segregado para os serviços contratados pela Claro;

b) Controlar e restringir os acessos de outras redes para a rede exclusiva utilizada na prestação do serviço, através de regras restritivas de firewall;

c) Prover, quando solicitado pela Claro, diagramas físicos e lógicos atualizados das redes que suportam as operações que são objeto do contrato, contendo os equipamentos utilizados e suas interconexões;

d) Prover monitoramento de segurança do tráfego de rede;

e) Implementar regras de controle de comunicação com a internet de acordo com a necessidade da operação;

f) Criar perfis de acessos para sistemas internos relacionados às operações, obedecendo aos princípios de mínimo privilégio e segregação de funções;

g) Proteger as conexões de rede da CONTRATADA de outras redes externas, de acordo com as melhores práticas de Segurança da Informação;

h) Os ativos da CONTRATADA devem prover proteção contra códigos maliciosos, tais como antivírus e personal firewall (manter atualizados diariamente);

i) A instalação e utilização de pontos de acesso sem fio (padrão IEEE 802.11) deve ser controlada. A interface de administração de equipamentos de rede, computadores e pontos de acesso sem fio deve ser acessada somente por usuários autorizados;

j) Os pontos de acesso sem fio devem ser configurados conforme padrões seguros de comunicação (Ex:WPA2 ou superior);

k) Os ativos envolvidos na prestação do serviço para a Claro devem ser contemplados por um processo de blindagem (hardening);

l) Deve haver um método de backup das informações da Claro que deve ser testado e atualizado periodicamente;

m) Somente os protocolos e sites necessários para execução dos serviços contratados devem ser liberados para acessos dos usuários;

n) Desabilitar serviços e funcionalidades desnecessárias nos computadores e equipamentos de rede que suportam as operações da Claro;

o) Os servidores devem ser armazenados em locais seguros;

p) A CONTRATADA deve restringir o acesso físico aos pontos de rede acessíveis publicamente, pontos sem fio, gateways e dispositivos portáteis;

q) Os computadores devem ser bloqueados após 15 (quinze) minutos de inatividade e somente devem ser desbloqueados através da senha de acesso do usuário;

r) Os equipamentos envolvidos na operação devem possuir apenas conexões, interfaces, aplicações e dispositivos necessários à sua finalidade. O fornecedor de Call Center deve bloquear a utilização de dispositivos que permitam a gravação de informações em mídia, como por exemplo:

- CD RW
- DVD RW
- Computadores de mão
- Câmeras digitais e qualquer outro tipo de equipamento que contenha recursos de fotografia
- Telefones celulares com câmeras
- iPods
- Tablets
- Gravadores
- Filmadoras
- Pen drives
- Quaisquer outras mídias ou periféricos que possibilitem a gravação de informações

s) **Os dispositivos moveis estão autorizados somente para o uso de 2FA (Segundo Fator de Autenticação);**

t) Apresentar os requisitos de segurança lógica atualmente implementados na sua operação, bem como projetos de melhorias já em execução;

u) O sistema de gravação de áudio utilizado na prestação do serviço para a Claro deve estar em ambiente controlado de acesso restrito.

4.12. Segurança Física, Eletrônica e de PCI

i. Para as operações instaladas em sites de propriedade da CONTRATADA, esta deve atender aos requisitos de segurança física definidos pela Gerência de Segurança Física da Claro.

4.13. Testes de Segurança

i. A CONTRATADA deve permitir que a área de Segurança da Informação da Claro (ou terceiro por ela designado) realize os testes de segurança necessários quando solicitado em sistemas, sites, aplicações etc. (objetos do contrato);

ii. O resultado do teste será enviado a CONTRATADA que deverá retornar um plano de ação no prazo de 30 (trinta) dias informando os prazos para correção das vulnerabilidades identificadas.

4.14. Diligências de Conformidade

i. A CONTRATADA obriga-se a manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições abaixo exigidas:

a) A CONTRATADA deverá responder aos reportes e envio de evidências solicitadas pela Gerência de Segurança da Informação Corporativa da Claro, contendo autoavaliação (self-assessment) dos requisitos de segurança determinados em contrato;

b) Ambientes físicos e lógicos de recebimento, tratamento e manipulação de dados/informações objetos do contrato poderão passar por vistorias de segurança periódicas designadas pela Gerência de Segurança da Informação Corporativa da Claro;

c) Permitir que colaboradores da Claro, a qualquer tempo, possam proceder à verificação na CONTRATADA de conformidade dos controles incluídos no contrato, bem como permitir a análise e verificação de seus procedimentos de atendimento e habilitação dos serviços;

d) As não conformidades identificadas devem ser corrigidas e um Plano de Ação deverá ser enviado à Claro com prazo para regularização. Vulnerabilidades classificadas como ALTA, conforme metodologia própria de análise de riscos da Claro não poderão ser corrigidas num prazo superior a 30 (trinta) dias.

5. ENCERRAMENTO DO CONTRATO DE SERVIÇOS

i. A substituição ou mesmo o encerramento dos serviços contratados pode ocorrer a qualquer momento. Para isto, alguns itens de segurança devem ser atendidos:

a) Notificação de rescisão e/ou elaboração de termo de distrato e quitação, caso encerramento amigável;

b) Garantia da revogação dos acessos;

c) Destruição dos dados armazenados, demonstrados pela CONTRATADA, quando solicitado;

d) Entrega de todas as gravações telefônicas e logs armazenados pela CONTRATADA;

e) Revisão dos planos de continuidades de negócio que envolvam a CONTRATADA;

f) Prazo para que sejam feitas as devidas regularizações, devendo estar previsto em contrato;

g) Atualização de normas e processos que envolvam a CONTRATADA.

ii. A área da Segurança da Informação Corporativa ou, na impossibilidade desta, um terceiro contratado, poderá realizar diligência para verificar se as cláusulas do contrato estão sendo atendidas, principalmente aqueles referentes à destruição das informações e revogação dos acessos.

6. DISPOSIÇÕES FINAIS

a) A CONTRATADA deve preservar a informação e os ativos da CLARO, utilizando-os estritamente para o cumprimento de suas funções e cumprindo com as políticas, normas de segurança e procedimentos definidos para a operação do objeto contratado.

b) A CONTRATADA é responsável por qualquer fraude originada pelo não cumprimento dos procedimentos definidos, independentemente da existência de travas sistêmicas.

c) Os recursos colocados à disposição pela CLARO, incluindo sistemas, aplicações e aplicativos, deverão ser utilizados para propósitos relacionados com o objeto contratado, sendo proibida qualquer utilização dos recursos para fins ilegais e/ou lucrativos bem como comerciais ou profissionais diferentes aos permitidos pela empresa.

d) A CONTRATADA deve notificar o antes possível, sobre a ocorrência de incidentes ou eventos suspeitos que afetem ou possam afetar a segurança da informação e do negócio, mediante os procedimentos e canais definidos pela CLARO.

e) Está proibido tirar proveito das vulnerabilidades ou debilidades que porventura existem nos sistemas.

f) A CONTRATADA deve possuir solução tecnológica que integre/autentique o atendente em nossos sistemas/aplicações.

g) A CONTRATADA não deve utilizar qualquer tipo de solução de robotização ou mesmo Front-End únicos para acessar nossos sistemas/aplicações.

ANEXO I – ORIENTAÇÕES DE DESENVOLVIMENTO SEGURO DE SISTEMAS

1. REQUISITOS DE SEGURANÇA PARA DESENVOLVIMENTO SEGURO

Para garantir as premissas básicas de segurança da informação (confidencialidade, integridade e disponibilidade) devem ser utilizados controles de segurança adequados nos sistemas, aplicações e ou aplicativos que manipulem ou armazenem informações de propriedade da Claro.

1.1. Arquitetura de Segurança

O objetivo da arquitetura de segurança é definir algumas premissas de segurança relacionadas à infraestrutura de rede e detalhes operacionais importantes para garantir a segurança do sistema:

a) Os sistemas desenvolvidos devem seguir o modelo três camadas – Camada de Apresentação, Aplicação e Banco de Dados, segmentadas logicamente, com pelo menos a Camada de Apresentação separada fisicamente da Camada de Banco de Dados, ou seja, cada uma em um servidor.

b) Para aplicativos voltados ao público, acessíveis através de redes externas, estes devem estar segregados da rede interna para evitar o comprometimento do ambiente, portanto esses aplicativos devem ser implementados na DMZ.

c) Sistemas que possuam a necessidade de sair para internet para buscar alguma atualização, estes devem ser liberados no proxy de aplicação e restrito para URLs específicas.

d) O projeto deve contemplar um desenho lógico atualizado detalhando: os componentes da solução e uma breve descrição deles; o fluxo de comunicação entre os componentes da solução com uma breve descrição.

e) As liberações de portas de comunicação devem ser aprovadas pela Claro antes de serem configuradas.

f) Sistemas internos devem ser restritos à rede interna.

g) O sistema deve ser compatível com as regras de segurança definidas para infraestrutura dos servidores que hospedarão o sistema.

h) Softwares de prateleiras devem seguir os requisitos de desenvolvimento seguro descritos. Eles devem ter o mínimo de privilégio possível para executar suas funções, sendo restrito o acesso de administrador do sistema operacional.

i) Todos os canais humanizados, ou seja, aqueles que possuem interação com o usuário, devem possuir certificado HTTPS. Para canais externos estes certificados devem ser reconhecidos por uma CA externa, para internos é aceitável o uso de uma CA interna.

j) Informações sensíveis devem trafegar através de uma conexão criptografada e de maneira segura.

k) Nos servidores de desenvolvimento, homologação e produção devem ser removidos serviços desnecessários, como scripts, drivers, recursos, subsistemas e sistemas de arquivo desnecessários.

l) Não deve ser instalado plug-ins ou ferramentas não homologados no ambiente; em caso de necessidade, é necessário alinhar com a Claro (Segurança da Informação Corporativa) previamente.

m) Não deve ser utilizado componentes desatualizados ou sem suporte para compor a aplicação.

n) É obrigatório ter ambiente de homologação funcional, antes que o sistema seja portado para o ambiente de produção.

o) O sistema desenvolvido deve identificar requisitos de alta disponibilidade.

p) Interfaces administrativas, aquelas utilizadas para manutenção da aplicação, devem estar restritas à rede interna.

q) O projeto deve apontar as informações que necessitam ser contempladas no processo de *backup* existente.

r) Todos os projetos devem contemplar um plano de contingência para o sistema.

s) Todos os projetos de desenvolvimento de sistemas, aplicações e/ou aplicativos devem prever testes e controles para prevenção das principais ameaças (TOP 10 OWASP):

A1 -Injeção

A2 - Quebra de Autenticação e Gestão de Sessão

A3 -Exposição de Dados Sensíveis

A4 -Entidades Externas de XML (XXE)

A5 -Quebra de Controlo de Acessos

A6 -Configurações de Segurança Incorretas

A7 -Cross-Site Scripting (XSS)

A8 -Desserialização Insegura

A9 -Utilização de Componentes Vulneráveis

A10 -Registo e Monitorização Insuficiente

1.2. Práticas Gerais de Codificação

O objetivo é assegurar que dados confidenciais sejam acessíveis somente a usuários autorizados:

a) Utilize APIs que embutem tarefas específicas para realizar tarefas do sistema operacional. Não permitir que a aplicação execute comandos diretamente no sistema operacional, especialmente através da utilização de shells de comando iniciados pela aplicação.

b) Utilize mecanismo de verificação de integridade por checksum ou hash para verificar a integridade do código interpretado, bibliotecas, arquivos executáveis e arquivos de configuração.

c) Proteja as variáveis compartilhadas e recursos contra acessos concorrentes inapropriados.

d) Não se deve armazenar senhas ou chaves no código fonte.

e) As aplicações devem ser desenvolvidas para serem executadas com o mínimo de privilégio.

f) Não repasse diretamente dados fornecidos pelo usuário para qualquer função de execução dinâmica, sem antes realizar o tratamento dos dados de modo adequado (veja seção CRITÉRIOS PARA A CRIAÇÃO DE PERFIS DE ACESSO).

g) Revise todas as aplicações secundárias, códigos e bibliotecas de terceiros para determinar a necessidade do negócio e validar as funcionalidades de segurança, uma vez que estas podem introduzir novas vulnerabilidades.

h) Implemente atualizações de modo seguro. Se o sistema deve realizar atualizações automáticas, então utilize mecanismos de assinatura digital para garantir a integridade do código e garanta que os clientes façam a verificação da assinatura após o download. Use canais criptografados para transferir o código a partir do host do servidor.

i) Desabilite a funcionalidade de lembrar a senha (autocomplete) nos campos de senha do navegador.

1.3. Credenciais de Conta de Usuário

Toda credencial de acesso para sistemas internos, deve estar de acordo com o documento elaborado justamente para esse fim (Norma de Acesso Lógico a Recursos Informatizados).

Para os sistemas externos deve se utilizar esta guia de ORIENTAÇÃO TÉCNICA PARA DESENVOLVIMENTO SEGURO.

1.3.1. Autenticação

a) As informações referentes a uma credencial de acesso devem ser mantidas, mesmo após sua desativação, para que não seja perdido o histórico ou logs dela.

b) Os sistemas devem prever a criação de perfis de usuários integrados aos sistemas de autenticação homologados e em uso pela Claro, tendo seu controle de acesso centralizado pela área responsável pelo Controle de Acesso.

c) As credenciais do sistema devem ser armazenadas em um banco de dados com as informações criptografadas.

d) Deve-se exigir uma nova autenticação dos usuários antes da realização de operações críticas. Utilizar autenticação de múltiplos fatores para contas ou aplicações altamente sensíveis ou de alto valor financeiro.

e) Todos os sistemas, aplicações e/ou aplicativos que necessite de manutenção e esteja exposto na Internet devem utilizar dois fatores de autenticação (ex: Mobile Token).

f) Validar os dados de autenticação somente ao término de todas as entradas de dados, especialmente para as implementações de autenticação sequencial.

g) As respostas de falhas de autenticação não devem indicar qual parte dos dados de autenticação estão incorretos. Por exemplo: em vez de exibir mensagens como “Nome de usuário incorreto” ou “Senha incorreta”, apenas utilize mensagens como: “Usuário e/ou senha inválidos”, para ambos os casos de erro. As respostas de erro devem ser literalmente idênticas nos dois casos.

h) Os processos de redefinição de senhas e operações de mudanças devem exigir os mesmos níveis de controle previstos para a criação de contas e autenticação.

i) Exigir a mudança de senhas temporárias na próxima vez que o usuário realizar a autenticação no sistema.

j) Caso for utilizar código de terceiros para realizar a autenticação, é necessário que a Claro, através da Segurança da Informação, inspecione código para garantir se ele não é afetado por qualquer código malicioso.

1.3.2. Autorização

a) Os projetos dos sistemas devem prever sua utilização por usuários com credenciais de acesso que possuam o mínimo privilégio necessário para exercer sua função, não devendo haver a necessidade de aumento dos privilégios destes usuários para a execução delas.

b) O usuário de aplicação utilizado para autenticação com o banco de dados deve ser identificado pelo projeto, deve ter restrições quanto ao uso da rede e deve ser bloqueado para qualquer outro acesso.

c) Todos os acessos dos sistemas aos bancos de dados devem ser feitos através de uma camada intermediária, utilizando recursos como store procedures, views, componentes COM+, Web Services, Enterprise Services, Remote, NET e/ou outros recursos que garantam a segurança do acesso.

1.4. Critérios para Criação de Perfis de Acesso

a) Nomenclatura do perfil funcional:

- O nome do perfil deve refletir a função de negócio associada a ele, deixando clara a finalidade do perfil para quem visualizar seu nome. Exemplo: INCLUSÃO DE PACOTES TV, INCLUSÃO DE PACOTES INTERNET, ALTERAÇÃO DE ENDEREÇO.

b) Estrutura de autorização de acessos:

- Os sistemas devem, em sua estrutura de autorização de acessos, atender aos níveis de função, perfis funcionais e funcionalidades, conforme o exemplo:

LOCAL	FUNÇÃO	PERFIL FUNCIONAL	FUNCIONALIDADE SISTÊMICA
CALLCENTER	ATENDIMENTO MASSIVO	ALTERA ENDEREÇO	TELA DE CONSULTA AO CADASTRO

c) Função:

- Cada função deve ser composta apenas e pelos perfis funcionais pertinentes ao cumprimento das suas atividades. Os usuários do sistema devem receber seus privilégios ao serem vinculados a uma função.

d) Perfil funcional:

- Cada perfil funcional deve ser composto pelas funcionalidades sistêmicas pertinentes à função de negócio definida. Todo perfil deve ser criado considerando o conceito de "privilégio mínimo", ou seja, deve possuir a menor quantidade possível de acessos às funcionalidades sistêmicas necessárias para desempenhar uma atividade (função) de negócio.

e) Funcionalidades sistêmicas:

- Todas as funcionalidades sistêmicas devem estar associadas a algum perfil funcional. Uma mesma funcionalidade pode ser associada a vários perfis.

1.5. Tratamento de Erros e Trilhas de Auditoria (Logs)

a) Não exponha informações sensíveis nas respostas de erros, inclusive detalhes de sistema, tecnologias, identificadores de sessão ou informação da conta do usuário.

b) Use mecanismos de tratamento de erros que não exibam informações de debug ou informações da pilha de exceção.

c) Mensagens de erro padrão Claro deve ser exibido ao cliente. Utilizar o código de redirecionamento (3XX), que indica que algo mais precisa ser feito ou precisou ser feito para completar a solicitação;

d) O tratamento de erros lógicos associados com controles de segurança deve por padrão negar o acesso.

e) Todos os controles de log devem ser implementados em um sistema apartado da aplicação.

f) Adicionalmente, todos os sistemas devem incluir trilhas de auditoria.

g) O acesso e a leitura dos arquivos de logs devem ser restritos aos usuários autorizados.

h) Dados confidenciais utilizados na autenticação das credenciais de acesso (senhas, chaves privadas etc.) ou na autorização dos acessos (identificações ou senhas de sessão etc.) não devem ser registrados nos arquivos de log.

i) O sistema, aplicação e/ou aplicativo deve registrar, pelo menos, os seguintes eventos, quando aplicável: acesso a dados sensíveis, ações de usuários administrativos, acesso às trilhas de auditoria, tentativas de acesso inválidas, utilização dos mecanismos de autenticação e identificação, inicialização do registro de auditoria, falhas de validação de dados de entrada, tentativas de conexão com tokens de sessão inválidos ou expirados, falhas de conexão TLS com o backend e falhas de criptografia.

j) O sistema deve prover, pelo menos, os seguintes registros para cada entrada no log: identificação do usuário, tipo de evento, data e hora, indicação de sucesso ou falha, origem do evento e identificação do dado, componente, recurso ou objeto relacionado.

k) Utilizar uma função de hash criptográfica para validar a integridade dos registros de log.

1.6. Validação de Entradas

a) Todos os pontos de entrada de dados devem ser identificados no projeto.

b) Todos os parâmetros e dados de entrada, incluindo campos de formulário, campos ocultos (hidden), sequências de caracteres de consulta, cookies e cabeçalhos HTTP, devem ser validados pelo menos por:

- Tipo;
- Tamanho;
- Existência de caracteres inválidos;
- Formato;
- Intervalo.

c) Validar tipos de dados esperados, intervalo de dados, comprimento dos dados e sempre que possível validar todos os dados de entrada através de um método baseado em "lista branca / whitelist" que utiliza uma lista de caracteres ou expressão regular que define os caracteres permitidos.

d) Todos os dados enviados pelos usuários devem ser validados no servidor.

e) A rotina de validação de dados de entrada deve ser centralizada no sistema.

f) Decisões de segurança devem ser tomadas no servidor e não devem depender de dados de perfil ou permissões fornecidas diretamente pelo cliente (em aplicativos Web, isto inclui variáveis em cookies, campos ocultos de formulário, parâmetros GET ou POST e similares).

g) Deve-se implementar controles que inibam a entrada de dados ou scripts na URL.

h) Especificar conjunto de caracteres apropriados, como UTF-8, para todas as fontes de entrada de dados.

i) Codificar os dados para um conjunto de caracteres comuns antes da validação (Canonicalize).

j) Realizar o tratamento (sanitização), baseado em contexto, de todos os dados provenientes de fontes não confiáveis usados para construir consultas SQL, XML e LDAP.

k) Se qualquer caractere potencialmente 'perigoso' precisa ser permitido na entrada de dados do sistema, certifique-se que foram implementados controles adicionais como codificação dos dados de saída, APIs especificas que fornecem tarefas seguras e trilhas de auditoria no uso dos dados pelo sistema. A seguir, como exemplo de caracteres “potencialmente perigosos”, temos: <, >, ", ', %, (,), &, +, \, \', \".

l) Se a rotina de validação padrão não aborda as seguintes entradas, então elas devem ser verificadas discretamente:

- Verificar bytes nulos (%00).
- Verificar se há caracteres de nova linha (%0d, %0a, \r, \n).
- Verificar se há caracteres ponto-ponto barra (../ ou ..\) que alteram caminhos. Nos casos de conjunto de caracteres que usam extensão UTF-8, o sistema deve utilizar representações

alternativas como: %c0%ae%c0%ae/. A canonicalização deve ser utilizada para resolver problemas de codificação dupla (double encoding3) ou outras formas de ataques por ofuscação.

1.7. Configuração de Sistema

a) A aplicação não deve ser instalada utilizando parâmetros padrões como: caminhos e nome de diretórios, senhas, nome ou chave de usuários, dataset, entre outros.

b) Os canais de comunicação para administração remota devem ser protegidos.

c) Utilizar apenas requisições POST para transmitir credenciais de autenticação. Não expor os identificadores de sessão em URLs, mensagens de erro ou logs. Os identificadores de sessão devem apenas serem localizados no cabeçalho do cookie HTTP. Por exemplo, não trafegar os identificadores de sessão na forma de parâmetros GET.

d) Utilizar mecanismos complementares ao mecanismo de gerenciamento de sessão padrão para operações sensíveis do lado do servidor, como é o caso de operações de gerenciamento de contas, através da utilização de tokens aleatórios ou parâmetros associados à sessão. Este método pode ser usado para prevenir-se de ataques do tipo Cross Site Request Forgery.

e) Utilizar mecanismos complementares ao gerenciamento de sessão para operações altamente sensíveis ou críticas utilizando tokens aleatórios ou parâmetros em cada requisição.

f) Configurar o atributo "secure" para cookies transmitidos através de uma conexão TLS.

g) Configurar os cookies com o atributo HttpOnly, a menos que seja explicitamente necessário ler ou definir os valores dos cookies através de scripts do lado cliente do sistema.

h) Use o campo “referer” do cabeçalho somente como forma de verificação suplementar. Ele não deve ser usado sozinho como forma de checagem de autorização, pois o valor deste campo pode ser adulterado.

i) Não disponibilizar Servlets que controlem através de parâmetros, credenciais de acesso e regras de navegação.

j) Desabilitar a funcionalidade de *autocomplete* nos formulários que contenham informações sensíveis, inclusive no formulário de autenticação.

k) Desabilitar o cache realizado no lado cliente das páginas que contenham informações sensíveis. O parâmetro Cache-Control: no-store, pode ser usado em conjunto com o controle definido nos cabeçalhos HTTP “Pragma: no-cache”, que é menos efetivo, mas é compatível com HTTP/1.0.

l) Desabilitar a listagem de diretórios.

m) Prevenir a divulgação da estrutura de diretórios impedindo que robôs de busca façam indexação de arquivos sensíveis, através da correta configuração do arquivo robots.txt, definindo diretórios que devem ser inacessíveis a estes indexadores em um diretório subjacente isolado. Assim, o acesso ao diretório pai definido no arquivo robots.txt deve estar desabilitado em vez de desabilitar cada diretório individualmente.

n) Desativar os métodos HTTP desnecessários, como extensões WebDAV. Caso for necessário o uso de algum método HTTP estendido para suportar manipulação de arquivos, então utilize algum mecanismo de autenticação bem controlado.

o) Remover informações desnecessárias presentes nos cabeçalhos de resposta HTTP que podem estar relacionadas ao sistema operacional, versão do servidor web e frameworks de aplicação.

p) Implementar WS-Security que é uma extensão do SOAP para aplicar segurança a serviços da Web.

1.8. Criptografia

a) Todos os dados e informações devem ser tratados de acordo com os critérios oficiais de Classificação da Informação da Claro.

b) A utilização de chaves criptográficas deve ser controlada por ferramentas de mercado e formalizada.

c) A utilização da chave como aplicação e finalidade devem ser documentadas.

d) As chaves criptográficas devem ser fornecidas somente ao pessoal autorizado, e mediante autorização formal do proprietário da informação.

e) As chaves criptográficas utilizadas devem ser armazenadas em um local seguro, de forma que somente o pessoal autorizado pela área responsável tenha acesso.

f) Deve-se preferir a utilização de módulos de criptografia compatíveis com a FIPS 140-2 ou padrão equivalente para as operações de gerenciamento e utilização de chaves criptográficas.

g) Chaves utilizadas para criptografar outras chaves, também conhecidas como key encryption keys devem ser ao menos tão robustas quanto às chaves protegidas por elas.

h) O sistema deve ter mecanismos para prevenir a substituição não autorizada de chaves criptográficas.

i) Todos os softwares, funções e bibliotecas de criptografia utilizados nos sistemas devem ter sido previamente homologados e aprovados pelas áreas responsáveis na Claro.

j) Todas as chaves criptográficas deverão ser trocadas periodicamente através de cerimônia de alteração de chaves.

1.9. Gerenciamento de Sessão

a) Protocolos com criptografia, como HTTPS/TLS, devem ser usados para proteger dados confidenciais transmitidos através da rede.

b) Utilize controles de gerenciamento de sessão baseados no servidor ou em framework. O sistema deve reconhecer apenas os identificadores de sessão como válidos.

c) A criação dos identificadores de sessão deve ser sempre realizada em um sistema confiável, por exemplo: centralizar todo controle no servidor.

d) Usar algoritmos adequados que garantam a aleatoriedade dos identificadores de sessão.

e) A funcionalidade de logout deve encerrar completamente a sessão ou conexão associada.

f) A sessão deve ser limitada a no máximo 15 minutos de inatividade.

g) Se uma sessão estava estabelecida antes do login, então esta sessão deve ser encerrada para que uma nova sessão seja estabelecida após o login.

h) Gerar um novo identificador de sessão quando houver alguma nova autenticação.

i) Não permitir conexões simultâneas com o mesmo identificador de usuário.

j) Gerar um novo identificador de sessão e desativar o antigo identificador periodicamente. Isto pode mitigar certos cenários de ataques de sequestro de sessão (session hijacking), quando o identificador de sessão original é comprometido.

k) O estado de sessão deve ser protegido contra acesso não autorizado.

1.10. Controle de Acesso – Controles Sistêmicos

a) Utilizar apenas objetos do sistema que sejam confiáveis, como ocorre com os objetos de sessão do servidor, para realizar a tomada de decisões de autorização de acesso.

b) Utilize um único componente em todo o sistema para realizar o processo de verificação de autorização de acesso. Isso inclui bibliotecas que invocam os serviços externos de autorização.

c) Negar todos os acessos caso o sistema não consiga ter acesso às informações contidas na configuração de segurança.

d) Garantir os controles de autorização em todas as requisições, inclusive em scripts do lado do servidor, "includes" e requisições provenientes de tecnologias do lado cliente.

e) Restringir o acesso às funções protegidas, referência direta a objetos, serviços e dados do sistema somente aos usuários autorizados.

f) Restringir o acesso aos atributos e dados dos usuários, bem como informações das normativas usadas pelos mecanismos de controle de acesso.

g) Restringir o acesso às configurações de segurança relevantes apenas para usuários autorizados.

h) Limitar o número de transações que um único usuário não robotizado, através de CAPTCHA ou algum controle que determina um tempo às tentativas de acesso.

i) Se for permitida a permanência de sessões autenticadas e ativas por longos períodos, fazer revalidação periódica da autorização do usuário para garantir que seus privilégios não foram modificados e caso forem, realize o registro em log do usuário e exija nova autenticação.

1.11. Proteção de Dados

a) Dados confidenciais, dados pessoais, dados pessoais sensíveis de colaboradores/terceiros armazenados em banco de dados devem ser criptografados.

b) Um mecanismo de controle transacional no banco de dados (Commit/Rollback) deve ser contemplado.

c) O roteamento das conexões para o banco de dados deve ser sempre a partir da camada de aplicação, nunca deve existir nenhum computador de usuário, desenvolvedor ou suporte conectado diretamente ao banco de dados em sistemas de produção.

d) O processo de desenvolvimento e homologação dos sistemas deve ser realizado somente com bases de dados mascaradas e/ou dados fictícios, porém deve ser mantida a mesma estrutura das bases originais de produção e volume de dados suficientes para a execução dos testes, visando realizar simulações compatíveis à realidade do negócio.

e) Não armazenar senhas, strings de conexão ou outras informações confidenciais em texto claro ou em qualquer forma insegura no lado cliente.

f) Remover aplicações desnecessárias e documentação do sistema que possam revelar informações importantes para os agentes maliciosos.

g) O sistema deve dar suporte à remoção de dados confidenciais, dados pessoais, dados pessoais sensíveis quando eles não forem mais necessários.

h) Os métodos de mascaramento e anonimização devem ser realizados na origem dos dados (backend) ao invés do frontend;

i) Todo sistema deve entregar o menor número de informações possível, e quando se tratar de uma API que preveja reuso por demais consumidores que necessitem de mais informações, deve ser feito esforço razoável para balancear reusabilidade e risco. Pode ser necessária a criação de fluxos de restrição de informação condicionado ao consumidor;

j) Nenhuma credencial pode estar presente em URIs, exceto se tratar de um "app key" público, ou seja, usado apenas para fins de analítica e troubleshoot ao invés de autenticação;

k) As URIs não podem conter informações pessoais ou identificáveis dos usuários exceto se forem URIs de APIs, as quais precisam ser autenticadas;

1.12. Segurança nas Comunicações

a) Utilizar criptografia na transmissão de todas as informações sensíveis. Isto deve incluir TLS (última versão segura e estável) para proteger a conexão e deve ser complementado por criptografia de arquivos que contém dados sensíveis ou conexões que não usam o protocolo HTTPS.

b) Os certificados TLS devem ser válidos, possuir o nome de domínio correto, não estarem expirados e serem instalados com certificados intermediários, quando necessário.

c) Quando ocorre falha nas conexões TLS, o sistema não deve retornar uma conexão insegura.

d) Utilizar um padrão único de implementação TLS que é configurado de modo apropriado.

e) Especificar a codificação dos caracteres para todas as conexões.

1.13. Conformidade de Sistema

a) Garantir que os servidores, frameworks e componentes do sistema estão executando a última versão aprovada.

b) Garantir que os servidores, frameworks e componentes do sistema possuam os patches mais recentes aplicados para a versão em uso.

c) Remover todas as funcionalidades e arquivos desnecessários.

d) Remover o código de teste ou qualquer funcionalidade desnecessária para o ambiente de produção, antes que seja realizada a implantação do sistema.

e) O armazenamento da configuração de segurança para o sistema deve ser capaz de ser produzida de forma legível para dar suporte à auditoria.

f) Implementar um sistema de controle de mudanças para gerenciar e registrar as alterações no código, tanto do desenvolvimento, como dos sistemas em produção. O controle de mudanças deve contemplar no mínimo a documentação do impacto, aprovação documentada de alteração pelas partes autorizadas, teste de funcionalidade para verificar se a alteração não tem impacto adverso sobre a segurança do sistema e procedimentos de reversão.

1.14. Segurança em Bases de Dados

a) Usar consultas e variáveis parametrizadas fortemente “*tipadas*”, ou seja, uma vez que a consulta foi parametrizada, está não deverá ser alterada.

b) Utilizar validação de entrada e codificação de saída e assegure a abordagem de meta caracteres. Se houver falha, o comando no banco de dados não deve ser executado.

c) Realizar a codificação (escaping) de meta caracteres em instruções SQL.

d) O sistema deve usar o menor nível possível de privilégios ao acessar o banco de dados.

e) Usar credenciais individuais para acessar o banco de dados. Não utilizar contas genéricas ou de administração para o acesso, por exemplo, admin, root ou sys.

f) As strings de conexão não devem ser codificadas na aplicação. A string de conexão deve ser armazenada em um arquivo de configuração separado em um sistema confiável e as informações devem ser criptografadas.

g) Usar procedimentos armazenados (stored procedures) para abstrair o acesso aos dados e permitir a remoção das permissões das tabelas no banco de dados.

h) Remover ou modificar todas as senhas padrão de contas administrativas. Utilizar senhas robustas (incomuns ou difíceis de deduzir) ou implementar autenticação de múltiplos fatores. Desabilitar qualquer funcionalidade desnecessária no banco de dados, como stored procedures ou serviços desnecessários. Instale o mínimo conjunto de componentes ou opções necessárias (método de redução da área de superfície).

i) Eliminar o conteúdo desnecessário incluído por padrão pelo fornecedor, ex: esquemas de exemplo.

j) Desabilitar todas as contas criadas por padrão e que não são necessárias para suportar os requisitos de negócio.

k) O sistema deve se conectar ao banco de dados com diferentes credenciais de segurança para cada tipo de necessidade, como: usuário, somente leitura, convidado, administrador etc;

l) os dados em repouso em provedores de nuvem precisam ser criptografados.

1.15. Gerenciamento de Arquivos

a) Solicitar autenticação antes de permitir que seja feito o upload e download de um arquivo.

b) Limitar os tipos de arquivos que podem ser enviados para aceitar somente os tipos que são necessários para os propósitos do negócio. Restringir o upload de arquivo de extensões do tipo: CMD, BAT, SCR, EXE, VBS e WS.

c) Validar se os arquivos enviados são do tipo esperado através da checagem dos cabeçalhos. Realizar a verificação de tipo de arquivo apenas pela extensão não é suficiente.

d) Desabilitar privilégios de execução nos diretórios de upload de arquivos.

e) No referenciamento de arquivos existentes, use uma lista branca (white list) de nomes e tipos de arquivos permitidos. Realize a validação do valor do parâmetro passado e caso não corresponda ao que é esperado, rejeite a entrada ou utilize um valor de arquivo especificado por padrão pela aplicação.

f) Não passar parâmetros de caminhos de diretórios ou arquivos nas requisições. Utilize algum mecanismo de mapeamento dos caminhos em disco para índices que são repassados para os usuários e servem para serem mapeados em uma lista pré-definida de caminhos dos arquivos.

g) Certificar-se de que os arquivos do sistema e os recursos são do tipo somente leitura.

h) Escanear arquivos que os usuários submeteram por mecanismo de upload em busca de ameaças digitais (Vírus, Ransomwares, Rootkits, entre outros).

1.16. Gerenciamento de Memória

a) Verificar se o buffer é tão grande quanto o especificado.

b) Ao usar funções que aceitam um determinado número de bytes para realizar cópias, como strncpy(), esteja ciente de que se o tamanho do buffer de destino for igual ao tamanho do buffer de origem, ele não pode encerrar a sequência de caracteres com valor nulo (null).

c) Verificar os limites do buffer caso as chamadas a função são realizadas em um loop e verificar se não há nenhum perigo de escrever além do espaço alocado.

d) Truncar todas as strings de entrada para um tamanho razoável antes de passá-las para as funções de cópia e concatenação.

e) Encerre os recursos de modo específico, sem contar com o garbage collector na liberação dos recursos alocados para objetos de conexão, identificadores de arquivo etc.

f) Usar pilhas não-executáveis, quando disponíveis.

g) Evitar o uso de funções reconhecidas por serem vulneráveis, por exemplo: printf, strcat, strcpy, etc.

h) Liberar a memória alocada de modo apropriado após concluir a sub-rotina (função/método) e em todos os pontos de saída.

2. SISTEMAS QUE MANIPULAM DADOS DE PORTADOR DE CARTÃO DE PAGAMENTO

a) Qualquer sistema que armazene, processe ou transmita dados de portador de cartão de pagamento de qualquer bandeira (marca) deve obrigatoriamente cumprir com os requisitos abaixo. Isto se faz necessário para evitar fraudes financeiras envolvendo os sistemas da Claro e para manter a conformidade com o padrão PCI-DSS.

b) Os requisitos abaixo são complementares aos citados anteriormente.

c) Os fornecedores e/ou serviços contratados pela Claro devem estar em conformidade com o padrão PCI-DSS. Para estes casos, o fornecedor deve sempre disponibilizar para a Claro o AOC - *Attestation of Compliance* ou a testado de conformidade.

2.1. Proteção de Dados

a) Dados confidenciais de autenticação do cartão de pagamento não devem ser armazenados após a autorização (mesmo se estiverem criptografados). Estes incluem:

i. Conteúdo completo de qualquer trilha magnética do cartão de pagamento;

ii. Código ou valor de verificação do cartão (o número de três ou quatro dígitos impresso na frente ou atrás do cartão de pagamento) usado para verificar as transações com cartão não presente, nominados CAV2/CVC2/CVV2/CID, dependendo da bandeira;

iii. PIN (personal identification number) ou o *PIN block*criptografado.

b) Mascarar o número do cartão (PAN) quando exibido (os primeiros seis e quatro últimos dígitos são o número máximo de dígitos a serem exibidos).

2.2. Criptografia

a) Caso seja necessário o armazenamento do número do cartão (PAN) e isto esteja na especificação do projeto, o armazenamento em texto claro é expressamente proibido, sendo permitido um dos métodos abaixo:

- Criptografia forte, com algoritmos de criptografia simétrica com chave igual ou maior que 128 bits e com gerenciamento adequado de chaves;
- Truncamento do número do cartão armazenando-se apenas os seis primeiros e quatro últimos dígitos do PAN;
- *Hashing* seguro aplicado sobre o PAN completo. Entende-se por *hashing* seguro a concatenação de um valor aleatório (*salt*) ao PAN antes da aplicação de uma função de *hash* matematicamente segura, como o SHA-1, tendo por objetivo a proteção contra-ataques que utilizem tabelas com valores pré-calculados de *hashes*.

b) Devem-se utilizar protocolos robustos de criptografia e de segurança (por exemplo, TLS/TLS, IPSEC, SSH, etc.) para proteger dados do portador de cartão de pagamento durante a transmissão por redes públicas, abertas (exemplos de redes abertas e públicas incluem, mas não se limitam, a: Internet, tecnologias sem fio, GSM, GPRS, 3G, etc.).

c) A geração de chaves criptográficas deve se dar apenas em módulos criptográficos ou em sistemas comprovadamente seguros, utilizando-se geradores de números aleatórios compatíveis com a Norma ISO 18031, ou então, caso seja utilizado uma rotina geradora de números pseudoaleatórios, deve-se garantir suficiente entropia para a semente utilizada.

d) Quando necessário, as chaves criptográficas devem ser distribuídas para os sistemas que as utilizarão através de métodos seguros, aplicando-se os conceitos de duplo controle e conhecimento dividido.

e) As chaves simétricas utilizadas para criptografar os dados de portador de cartão de pagamento devem ser substituídas após 3 anos de uso e os dados devem ser criptografados novamente com uma nova chave. Chaves assimétricas devem ser substituídas após 5 anos de uso.

f) Qualquer chave de criptografia utilizada para criptografar os dados de portador de cartão de pagamento deve ser imediatamente substituída se houver qualquer suspeita de seu comprometimento. As chaves também devem ser substituídas quando do desligamento de qualquer funcionário com conhecimento da chave ou de parte da chave.

g) Não utilizar algoritmo de criptografia própria.

2.3. Revisão de Código

a) Qualquer código (sistemas internos ou públicos) deve ser revisado antes da liberação para produção com o objetivo de identificar qualquer vulnerabilidade potencial de codificação.

b) A revisão de código deve ser realizada por outras pessoas, que não o autor que originou o código. O(s) revisor(es) deve(m) ter conhecimento de técnicas de análise de código e das práticas de codificação seguras.

c) As revisões devem garantir que o código foi desenvolvido de acordo com os requisitos descritos neste documento.

d) As correções necessárias devem ser implementadas antes da liberação do sistema para a produção.

e) Toda revisão de código deve produzir relatórios que descrevam o código revisado, as vulnerabilidades encontradas e as correções realizadas.

f) Os resultados das revisões de código devem ser revisados e aprovados pelo gerente do projeto antes da liberação.

g) Configurar os principais headers de segurança:

- Cross-origin resource sharing (CORS) - Mecanismo de navegador que permite o acesso controlado a recursos localizados fora de um determinado domínio;
- HTTP Strict Transport Security (HSTS) - Ajuda a prevenir que futuras conexões com este servidor não sejam criptografadas, dificultando assim ataques de downgrade;
- Content-Security-Policy (CSP) - Evita uma ampla variedade de ataques, incluindo scripts entre sites e outras injeções entre sites;

3. SISTEMAS PARA DISPOSITIVOS MÓVEIS

a) Qualquer sistema desenvolvido para plataformas móveis, como Android, IOS ou outros, deve obrigatoriamente cumprir com os requisitos abaixo. Isto se faz necessário para evitar a exploração de

vulnerabilidades comuns em aplicativos destas plataformas, que possuem características únicas em relação a sistemas desktops e aplicações web.

b) Os requisitos abaixo são complementares aos citados anteriormente e devem ser aplicados conforme a plataforma da aplicação.

3.1. Configuração de Sistema

a) Os valores exclusivos de identificação do dispositivo (Device ID) não devem ser usados como controle de segurança.

b) O aplicativo deve ser assinado com um certificado digital válido.

c) O aplicativo não deve armazenar chaves secretas ou senhas no seu código executável.

d) O aplicativo para uso interno, ou seja, para colaboradores deve desabilitar recursos de fotografia de tela como “print screen” ou “auto-snapshot”, para impedir que informações sensíveis possam ser divulgadas por esta funcionalidade.

e) O aplicativo não deve ser executado em um dispositivo com alterações em seu sistema operacional. Tradicionalmente estas técnicas são conhecidas como “Root Device” no caso de sistemas Android e “Jailbreaking” no caso de sistemas iOS.

f) As permissões e os arquivos requisitados pelo aplicativo para o seu correto funcionamento devem seguir o princípio de privilégio mínimo.

g) Os arquivos binários do aplicativo devem ser ofuscados para evitar ataques que utilizem técnicas de engenharia reversa do código.

h) Todos os dados de teste devem ser removidos do container do aplicativo (arquivos .apk, .ipa e .bar, entre outros formatos).

i) O aplicativo deve validar seus arquivos de configuração para avaliar se não foram alterados para inserir variáveis inseguras, como flags de depuração, permissões de leitura etc.

j) O aplicativo deve utilizar as mínimas permissões necessárias para seu funcionamento. Isto contribuiu para garantir a privacidade dos usuários e a usabilidade do sistema.

k) O aplicativo não deve criar arquivos com permissões globais no sistema de arquivos do dispositivo, como *MODE_WORLD_READABLE* ou *MODE_WORLD_WRITABLE*. Deve-se usar o princípio de privilégio mínimo para evitar que permissões excessivas concedidas a um aplicativo possam comprometer a segurança do dispositivo móvel.

l) O aplicativo deve manter em memória as credenciais de acesso (usuário e senha) o mínimo de tempo possível, apenas o suficiente para completar o processo de validação.

m) O aplicativo deve descartar e limpar toda a memória associada com os dados do usuário e todas as chaves mestras usadas para decifrar dados sensíveis.

n) O suporte ao JavaScript e aos Plugins devem estar desabilitados para quaisquer WebViews;

o) O sistema de acesso a arquivos deve estar desativado para quaisquer WebViews, como por exemplo, “webview.getSettings ()” e “setAllowFileAccess (false)”, impedindo que aplicações web possam acessar conteúdo local do aplicativo.

p) Todos os serviços devem filtrar completamente e validar as entradas vindas do aplicativo. Ao lidar com consultas dinâmicas ou “ContentProviders” deve-se garantir que estão sendo utilizadas consultas parametrizadas;

q) Deve-se restringir o uso do modo de depuração dos aplicativos evitando a fácil manipulação em tempo de execução por um atacante ou malware. Normalmente isto é possível com o uso da flag “debuggable = set false” em sistemas Android, por exemplo.

r) Deve-se invocar diretamente o aplicativo recebedor das chamadas e mensagens de sistemas, evitando o uso de recursos como a propagação (broadcast) de intents em sistemas Android ou App Extensions em sistemas iPhone.

s) O aplicativo deve implementar uma configuração padrão para o usuário o mais segura possível (buscando um equilibro entre segurança e usabilidade).

t) O aplicativo deve informar ao usuário sobre os possíveis riscos quando se mudam os parâmetros de segurança na configuração. Nestes casos, a opção padrão selecionada deve ser a mais restritiva do ponto de vista da segurança.

u) O aplicativo deve ser atualizado automaticamente nos dispositivos quando for necessário.

3.2. Gerenciamento de Sessão

a) O ID de sessão deve cumprir os seguintes requisitos:

- Altera e é diferente para cada login e autenticação válida do usuário;
- É removido após o processo de “LogOut” (desvinculação de dispositivos).

b) A sessão deve ser limitada a no máximo 15 minutos de inatividade.

c) A funcionalidade de logout deve encerrar completamente a sessão ou conexão associada.

d) Se uma sessão estava estabelecida antes do login, então esta sessão deve ser encerrada para que uma nova sessão seja estabelecida após o login.

e) Protocolos com criptografia, como HTTPS/TLS, devem ser usados para proteger dados confidenciais transmitidos através da rede.

f) Dados web trafegados pelo aplicativo, como tráfego via HTTPS, não devem ser armazenados, mesmo em arquivos de cache.

3.3. Proteção de Dados

a) O aplicativo deve validar os certificados de criptografia utilizados durante a transferência de dados.

b) O aplicativo deve utilizar TLS para todas as conexões que:

- Transmitam credenciais de autenticação ou tokens de sessão do usuário;
- Enviem ou recebam dados sensíveis ou acessem operações sensíveis;
- Estejam relacionadas com a administração da aplicação.

c) Não devem ser enviados dados sensíveis através de canais alternativos, tais como SMS, MMS ou notificações.

d) O aplicativo não dever armazenar dados sensíveis em recursos compartilhados do dispositivo, como por exemplo, diretórios compartilhados ou o cartão SD. Para sistemas Android o armazenamento local de informações no dispositivo deve utilizar a criptografia de arquivos locais usando "setStorageEncryption".

e) O aplicativo não deve armazenar dados sensíveis nos bancos de dados locais do dispositivo. Se algum dado necessitar de armazenamento este deverá usar técnicas de proteção, como truncamento, por exemplo. Isto vale mesmo se dados sensíveis forem armazenados com o uso de técnicas de criptografia, como o iOSKeychain ou em bases SQLite em sistemas Android.

f) O aplicativo não deve oferecer a possibilidade de autocomplete para dados sensíveis, como senhas, informações pessoais ou de cartão de crédito.

g) O aplicativo não deve permitir a exportação de atividades sensíveis executadas pelo aplicativo.

h) Aplicativos que trafegarem dados sensíveis devem usar técnicas de Certificate Pinning (Fixação de Certificado, em tradução livre) para impedir a interceptação do tráfego do aplicativo.

3.4. Autenticação e Gerenciamento de Senhas

a) Instâncias em que o aplicativo móvel exige que um usuário crie uma senha ou PIN (digamos, para acesso off-line), o aplicativo nunca deve usar um PIN, mas impor uma senha que siga uma política de senha forte.

b) Os dispositivos móveis também podem oferecer a possibilidade de usar dados biométricos para realizar a autenticação, que nunca deve ser usada devido a problemas com falsos positivos / negativos.

c) Limpe os locais da memória que contenham senhas diretamente depois que seus *hashes* foram calculados.

d) Com base no nível de risco do aplicativo móvel, considere utilizar a autenticação de dois fatores.

e) Para a autenticação do dispositivo, evite usar somente qualquer identificador fornecido pelo dispositivo (como UID ou endereço MAC) para identificar o dispositivo, mas aproveite os identificadores específicos do aplicativo, bem como do dispositivo (que idealmente não seria reversível).

f) Nos cenários em que é necessário acesso offline aos dados, adicione um atraso intencional de 2 segundos ao processo de entrada de senha após cada tentativa de entrada malsucedida.

g) Em cenários em que o acesso offline aos dados é necessário, deve ser realizado o bloqueio de conta / aplicativo e / ou dados de aplicativo após o número 10 de tentativas de senha inválidas.

h) Ao utilizar um algoritmo de hash, use apenas um padrão aprovado pelo NIST, como SHA-2.

i) Considerar sempre incluir informações de contexto (como local de IP etc.) durante os processos de autenticação para executar a detecção de anomalias de login.

j) Em vez de senhas, use tokens de autorização padrão da indústria (que expiram com a frequência possível) que podem ser armazenados com segurança no dispositivo (conforme o modelo OAuth) e que são limitados ao serviço específico.

k) Integrar uma solução CAPTCHA sempre que isso melhorar a segurança sem incomodar muito a experiência do usuário (como durante novos registros de usuários, postagem de comentários de usuários, pesquisas on-line, “entre em contato”, páginas de envio de e-mail etc.).

3.5. Ofuscação de Código

a) Ofuscar todo o código de aplicativo confidencial, executando um programa de ofuscação de código automatizado usando software comercial de terceiros ou soluções de código aberto.

b) Para aplicativos que contêm dados confidenciais, dados pessoais, dados pessoais sensíveis, devem ser implementadas técnicas de antidepuração (por exemplo, evite que um depurador/debug seja anexado ao processo*; android: debuggable = ”false”*).