

REQUISITO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

CONTRATAÇÃO DE SERVIÇOS DE TERCEIROS- WEBSITES EXTERNOS

CONTROLE DE VERSÃO :

Revisão	Data	Motivo	Responsável
00	*17.09.2020*	Versão Inicial	*Nilson Luiz Tedeschi / Paulo Quito*
01	*08.12.2024*	Atualização das normas ABNT, Inclusão do item 4.1 e 4.3.1 subitem "F" e atualizações nos itens 4.3.2 e 4.3.3	*Nilson Luiz Tedeschi / Paulo Quito / Carolina de Moraes Tiuzsi / Letícia Medeiros Mendes*

** Este documento está alinhado à **PL-SEG-023 antigo (NR-SEG-009) Requisitos de Segurança da Informação e de Privacidade para Contratação de Serviços de Terceiros***

SUMÁRIO

1. OBJETIVO 4
2. APLICAÇÃO 4
3. REFERÊNCIAS 4
4. REQUISITOS DE SEGURANÇA PARA CONTRATAÇÃO DE SERVIÇOS DE TERCEIROS – Websites Externos 5
4.1. Aspectos Gerais 5
4.2. Organização de Segurança da Informação e Proteção de Dados Pessoais 6
4.3. Desenvolvimento 7
4.3.1. Segurança para Sistemas Web 7
4.3.2. Identidade do Site / Aplicativo 14
4.3.3. Utilização de E-Mail ou E-Mail Marketing 16
4.3.4. Tempo de Armazenamento 17
4.4. Proteção de Dados 17
4.5. Testes de Segurança 18
4.6. Gestão de Vulnerabilidade 18
4.7. Segurança nas Aplicações/Aplicativos Móveis 18
4.8. Incidentes de Segurança e Privacidade 21
4.9. Diligências de Conformidade 22
4.10. Gestão de Continuidade de Negócios 22
4.11. Descarte 23
5. ENCERRAMENTO DO CONTRATO DE SERVIÇOS 23

1. OBJETIVO

Apresentar os requisitos de Segurança da Informação e Privacidade obrigatórios que deverão ser observados pela CONTRATADA, para desenvolver websites (sites) para anúncio, comercialização de produtos, serviços ou promoções, dentre outras necessidades que se façam necessárias, 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 27001:2022 Versão Corrigida:2023:** Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação – Requisitos;
- **ABNT NBR ISO/IEC 27002:2022:** Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação;
- **ABNT NBR ISO/IEC 27005:2023:** Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação;
- **ABNT NBR ISO/IEC 27701:2019:** Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes;
- **CÓDIGO DE ÉTICA**, do Grupo América Móvil;
- **CÓDIGO DE AUTORREGULAMENTAÇÃO PARA PRÁTICA DE E-MAIL MARKETING** (http://www.capem.org.br);
- **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.**
- **RESOLUÇÃO Nº 477, de 07.08.2007** – Aprova o Regulamento do Serviço Móvel Pessoal (SMP);
- **REGISTRO.BR** (https://registro.br).

4. REQUISITOS DE SEGURANÇA PARA CONTRATAÇÃO DE SERVIÇOS DE TERCEIROS – Websites Externos

4.1. Aspectos Gerais

i. Todos os requisitos de segurança indicados nesta política devem ser incluídos na Especificação Técnica pelas áreas requisitantes da contratação para envio à Diretoria de Compras visando à elaboração das RFPs;

ii. A manutenção dos requisitos de segurança, bem como seu fiel cumprimento é de responsabilidade exclusiva da CONTRATADA, por isso cabe a este instituir procedimentos regulares de inspeções e auditorias relacionadas à segurança da sua operação;

iii. A CONTRATADA deve apresentar recursos de segurança física e lógica que possibilitem a efetiva proteção da finalidade, necessidade, confidencialidade, integridade, disponibilidade e autenticidade das informações da Empresa, desde a fase de desenvolvimento até a efetiva entrega do site;

iv. Em linhas gerais, a CONTRATADA deve observar, considerar, implementar, manter, se comprometer e garantir alta qualidade para os recursos de segurança especificados no contrato ao longo de todo o desenvolvimento do site;

v. A Gerência de Segurança da Informação, pode, baseada no conteúdo desta política e demais normativos referentes à contratação de terceiros, recomendar a não contratação ou o término do vínculo com qualquer fornecedor;

vi. Para a verificação dos requisitos estabelecidos em contratos definidos com a CONTRATADA, a Empresa pode, a qualquer tempo, solicitar evidências, realizar entrevistas com os profissionais da CONTRATADA escolhido e realizar visitas técnicas;

vii. A Gerência de Segurança da Informação pode, a qualquer tempo e mediante prévio agendamento de, pelo menos, 3 (três) dias de antecedência, realizar visitas técnicas com o objetivo de avaliar as condições de segurança física e digital para aferição se os itens de segurança estão sendo contemplados e cumpridos em conformidade com o disposto no contrato firmado e seus anexos;

viii. Em caso de possíveis não conformidades apuradas numa visita técnica, a Empresa notifica a CONTRATADA estando este obrigado a apresentar justificativa imediata com solução para o problema, ou então adequar os pontos notificados em prazos previamente acordados a partir do recebimento da notificação, sendo que pontos críticos que representem risco iminente devem ser tratados e resolvidos imediatamente;

ix. O assunto não se esgota nesta política. Todas as áreas requisitantes de fornecedores de sites externos e aplicativos devem consultar normativos complementares e específicos sobre contratação de serviços de TI;

x. Os critérios e diretrizes aqui estabelecidos devem ser aplicados para novos contratos a partir da data de publicação desta política.

4.2. 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.

4.3. Desenvolvimento

i. A CONTRATADA deve garantir as premissas básicas de segurança da informação (finalidade, necessidade, confidencialidade, integridade, disponibilidade e autenticidade) para todos os sistemas, sites e/ou aplicações próprias ou que serão desenvolvidas para cumprimento do objeto do contrato que manipulem dados ou informações da Claro, seguindo e implementando os controles estabelecidos abaixo:

4.3.1. Segurança para Sistemas Web

A) Autenticação

i. Requerer autenticação para todas as páginas e recursos, exceto para aqueles que são intencionalmente públicos;

ii. Utilizar apenas requisições POST para transmitir credenciais de autenticação;

iii. Desabilitar a funcionalidade de lembrar a senha (autocomplete) nos campos de senha do navegador;

iv. Adicionar 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;

v. Definição de complexidade mínima na criação de senhas, sendo elas:

- Tamanho mínimo de 8 caracteres;
- Senha não deve começar com caractere de espaço;
- Senha deve conter caractere minúsculo;
- Senha deve conter caractere maiúsculo;
- Senha deve conter caractere numeral;
- Senha deve conter caractere especial.

vi. Solicitar a troca periódica da senha conforme o tratamento da norma de gestão de acesso da Claro, há cada 150 dias, não podendo ser reutilizado senhas antigas.

B) Validação de Entradas

i. Validar todos os dados provenientes dos clientes antes do processamento, incluindo todos os parâmetros, campos de formulário, consentimentos, conteúdo das URLs e cabeçalhos HTTP, por exemplo: nomes e valores dos cookies. Certificar-se também de incluir automaticamente mecanismos de postback nos trechos de código JavaScript, Flash ou qualquer outro código incorporado;

ii. Verificar os valores de cabeçalho, tanto das requisições, como das respostas, que contém apenas caracteres ASCII;

iii. Validar dados provenientes de redirecionamentos para evitar que conteúdo malicioso seja incluído diretamente para o alvo do mecanismo de redirecionamento, podendo assim contornar a lógica do sistema e qualquer validação executada antes do redirecionamento;

iv. Usar apenas referências de arquivos internos ou em servidores controlados pela equipe de segurança em páginas que utilizarem JavaScript.

C) Gerenciamento de Sessão

i. Definir o domínio e o caminho para os cookies que contém identificadores de sessão autenticados para um valor devidamente restrito para o site;

ii. Disponibilizar a funcionalidade de logout em todas as páginas que requerem autenticação;

iii. 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;

iv. Gerar um novo identificador de sessão caso a segurança da conexão mude de HTTP para HTTPS, como pode ocorrer durante a autenticação. Internamente à aplicação, deve utilizar HTTPS de forma constante em vez de alternar entre HTTP para HTTPS;

v. 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 deve ser usado para prevenção de ataques do tipo Cross Site Request Forgery;

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

vii. Configurar o atributo "secure" para cookies transmitidos através de uma conexão TLS;

viii. 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.

D) Controle de Acesso

i. Restringir o acesso às URLs protegidas somente aos usuários autorizados;

ii. 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;

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

E) Proteção de Dados

i. Os controles de segurança de informações e TI devem ser aplicados adequadamente a todos os aspectos do desenvolvimento do(s) site(s) para garantir que os dados sejam protegidos adequadamente;

ii. O princípio geral deve ser o de que todos os dados são adequadamente protegidos do ponto de recepção, passando pelo armazenamento, transferência, processamento e até a eliminação segura dos dados. Assim, as atividades para proteção de dados devem envolver:

   a) Remover comentários do código de produção que são acessíveis pelos usuários e podem revelar detalhes internos do sistema ou outras informações sensíveis;

   b) Não incluir informações sensíveis nos parâmetros de requisição HTTP GET;

   c) Desabilitar a funcionalidade de autocompletar nos formulários que contenham informações sensíveis, inclusive no formulário de autenticação;

d) 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;

e) Implementar política de privilégio mínimo, restringindo os usuários apenas às funcionalidades, dados e informações do sistema que são necessárias para executar suas tarefas;

f) Dados confidenciais armazenados em banco de dados devem ser criptografados;

g) Proteger o código-fonte presente no servidor para que não seja acessado por algum usuário;

h) Contemplar um mecanismo de controle transacional no banco de dados (Commit/Rollback);

i) Implementar roteamento das conexões para o banco de dados 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;

j) Realizar o processo de desenvolvimento e homologação dos sistemas 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;

k) Remover do aplicativo e/ou bases de dados as contas, IDs de usuário, senhas e dados de teste ou prova antes que ele se torne ativo ou seja instalado em produção;

l) Não armazenar senhas, strings de conexão ou outras informações confidenciais em texto claro ou em qualquer forma criptograficamente insegura no lado cliente. Aplicar também quando houver incorporação de formatos inseguros como: MS viewstate,
Adobe Flash ou código compilado que roda no lado cliente;

m) Remover aplicações desnecessárias e documentação do sistema que possam revelar informações importantes para os atacantes;

n) O sistema deve dar suporte à remoção de dados sensíveis quando estes não forem mais necessários, como, por exemplo: informação pessoal ou determinados dados financeiros.

F) Privacidade de Dados

i. Todos os aplicativos/sites devem estar registrados nas ferramentas de privacidade, ROPA (Recording of Processing Activities ou Registro de Atividades de Tratamento) da Empresa. Para aplicativos/sites existentes e PBD (Privacy by Design) para novos aplicativos/sites, o que deve incluir, no mínimo, as seguintes informações: (i) lista completa dos dados tratados; (ii) finalidades; e (iii) base legal a serem apreciadas e aprovadas pela Empresa; sempre observando a proporcionalidade dos dados coletados em razão da finalidade pretendida.

a) Após análise e determinação da base legal mais adequada a cada caso, e se for determinado o consentimento, que deve ser obtido por manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, o fornecedor deve utilizar da ferramenta técnica disponibilizada pela Empresa para a coleta dos consentimentos e assegurar o correto encaminhamento destes, garantindo que os titulares possuam ferramentas para revogar tais consentimentos a qualquer momento;

b) No caso de coleta de dados de menores, sejam de crianças ou adolescentes, o fornecedor garante, sob sua exclusiva responsabilidade, obter e gerenciar o consentimento dos responsáveis legais, sempre garantido o melhor interesse e conforme disposições legais aplicáveis;

c) Todos os aplicativos/sites desenvolvidos pelos fornecedores externos à Empresa devem ser registrados nos fluxos de tratamento de dados deste fornecedor, seja para desenvolvimento total, ou para fluxos específicos, como, por exemplo, no caso de cobilling;

d) O fornecedor deve apresentar, sempre que solicitado pela Empresa e sendo viável, o teste de ponderação LIA (Legitimate Interests Assessment), caso haja enquadramentos cuja base legal seja o legítimo interesse, bem como seu respectivo DPIA (Data Protection Impact Assessment), ou seja, o Relatório de Impacto à Proteção de Dados (RIPD);

e) O fornecedor assegura seguir todos os princípios destacados na LGPD, em seu artigo 6º) em especial os de finalidade, livre acesso, transparência, segurança e não discriminação.

ii. Sobre a política de privacidade:

a) Não sendo o aplicativo/site de propriedade e desenvolvimento interno da Empresa, o fornecedor deve possuir política de privacidade própria para o tratamento de dados pessoais e sensíveis, sendo que este deve observar, na medida da razoabilidade, as recomendações da Empresa para construção da sua política de privacidade própria, observando as seguintes premissas e evitando situações conflitantes com os termos da política de privacidade da Empresa: (i) a linguagem utilizada deve ser simples e/ou visual; (ii) a disponibilização de canais de atendimento ao titular e designação para contato com o Encarregado/DPO, e (iii) fácil acesso ao documento da política de privacidade;

b) Na Empresa, os aplicativos/sites próprios possuem por regra o link para o Portal de Privacidade da Claro, sendo que, no caso dos aplicativos, este link deve constar no app, bem como nas lojas e nos demais pontos de coleta de dados;

iii. A respeito dos direitos dos titulares:

a) Cabe aos fornecedores disponibilizar ferramentas para acesso ao canal de atendimento aos titulares de dados, observadas as diretrizes inclusive técnicas da Empresa permitindo o contato com o Encarregado/DPO e, se possível, outros mecanismos de exercício de direitos previstos na LGPD, como formulários de requisições, painéis de controle do titular, dentre outras facilidades;

b) Os contratos entre a Empresa e seus fornecedores devem especificar de forma pormenorizada o fluxo de notificações entre as partes e o atendimento aos direitos dos titulares.

iv. Para novos SDK/Cookies:

a) No caso de novos sdks/cookies ou alteração dos sdks existentes e em uso em nossas plataformas, o responsável pelo aplicativo/site deve acionar a área de Governança de Aplicativos/Analytics do COE Digital (governanca.apps@claro.com.br) para que se processem os devidos escaneamentos e avaliações para que se possa submeter a análise de PbD (Privacy by Design), seguida das devidas recomendações;

b) Todos os aplicativos/sites devem ser escaneados todas as vezes em que houver uma atualização a ser obrigatoriamente comunicada pelo fornecedor à área de Governança de Aplicativos/Analytics para a avaliação, em especial quanto a novos recursos e possíveis tratamento de dados, sendo que o responsável pelo aplicativo/site deve atualizar os fluxos existentes no ROPA (Record of Processing Activities) os registros das atividades de tratamento ou registrar novos fluxos via PbD;

c) Os fornecedores não podem utilizar ou sinalizar seus aplicativos/sites com o banner ou

modal de consentimento de cookies da Empresa;

d) As funcionalidades relacionadas à privacidade devem ser apresentadas de forma clara, transparente e prática pelos fornecedores.

v. Para exclusão após tratamento:

a) O fornecedor deve desenvolver e demonstrar à Empresa em um documento oficial para devida aprovação uma Tabela de Temporalidade, na qual deve constar: (i) o prazo de descarte de todos os dados utilizados para o desenvolvimento da atividade; (ii) meios de exclusão ou, no caso de anonimização, quais são os métodos utilizados; e (iii) legislações aplicáveis no caso de retenção por obrigações legais;

b) Garantia de implementação de eliminação dos dados pessoais ao término do tratamento ou a pedido do titular, observados os prazos legais de descarte, bem como as autorizações legais para manutenção dos dados.

G) Segurança nas Comunicações

i. Filtrar os parâmetros que contenham informações sensíveis, provenientes do HTTP refere, quando realizar apontamentos para sites externos;

ii. Utilizar criptografia na transmissão de todas as informações sensíveis, incluindo TLS para proteger a conexão e sendo complementado por criptografia de arquivos que contém dados sensíveis ou conexões que não usam o protocolo HTTP. Os certificados TLS devem ser válidos, possuir o nome de domínio correto, não estarem expirados e serem instalados com certificados intermediários, quando necessário;

iii. Não retornar uma conexão insegura quando ocorre falha nas conexões TLS;

iv. Utilizar conexões TLS para todo conteúdo que requer acesso autenticado ou manutenção da confidencialidade das informações sensíveis;

v. Utilizar um padrão único de implementação TLS que é configurado de modo apropriado;

vi. Especificar a codificação dos caracteres para todas as conexões.

H) Configuração de Sistema

i. Desabilitar a listagem de diretórios;

ii. Restringir os privilégios do servidor web, dos processos e das contas de serviços para o mínimo possível;

iii. 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;

iv. Definir quais métodos HTTP, Get ou Post, a aplicação irá suportar e se serão tratados de modo diferenciado nas diversas páginas do sistema;

v. Desativar os métodos HTTP desnecessários, como extensões WebDAV. Caso seja necessário o uso de algum método HTTP estendido para suportar manipulação de arquivos, utilizar algum mecanismo de autenticação bem controlado;

vi. Certificar-se, se o servidor processar tantas requisições HTTP 1.0 e 1.1, de que ambos são configurados de modo semelhante ou assegurar que qualquer diferença que possa existir seja compreendida (ex. manuseio de métodos HTTP estendidos);

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

viii. Os servidores e recursos relacionados devem ser capazes de funcionar em redes IPv6.

I) Gerenciamento de Arquivos

i. Não salvar arquivos no mesmo diretório de contexto do sistema web. Os arquivos devem ser armazenados no servidor de conteúdo ou na base de dados;

ii. Prevenir ou restringir upload de qualquer arquivo que possa ser interpretado pelo servidor web;

iii. Não transmitir sem nenhum tratamento os dados informados pelo usuário a redirecionamentos dinâmicos. Se isto for permitido, então o redirecionamento deverá aceitar somente URLs relativas e validadas;

iv. Nunca enviar o caminho absoluto do arquivo para o cliente.

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. As políticas de retenção de dados devem ser definidas, monitoradas e aplicadas.

J) Tratamento de Erros e Trilhas de Auditoria (Logs)

i. Todo o acesso deve ser auditável para identificar data, hora, atividade e pessoa responsável;

ii. Não expor informações sensíveis nas respostas de erros, inclusive detalhes de sistema, identificadores de sessão ou informação da conta do usuário;

iii. Usar mecanismos de tratamento de erros que não exibam informações de debug (depuração) ou informações da pilha de exceção;

iv. Retornar mensagens de erro genéricas ao cliente;

v. Tratar seus erros sem depender das configurações do servidor;

vi. Liberar a memória alocada de modo apropriado quando ocorrerem condições de erro;

vii. Tratar erros lógicos associados com controles de segurança por padrão “negar o acesso”;

viii. Implementar controles de log em um sistema confiável (neste caso o servidor);

ix. Incluir, adicionalmente, trilhas de auditoria em todos os sistemas para as funções de maior criticidade e relevância para o negócio. Estas funções deverão ser definidas pelas áreas responsáveis e o proprietário do sistema, quando necessário;

x. Não deverá existir nenhum processo ou função que altere ou apague qualquer registro da trilha de auditoria, salvo o script de retenção;

xi. O processo confidencial deve ser controlado por uma trilha de auditoria que forneça um registro completo e a responsabilidade individual pelo ciclo de vida dos ativos de informação para garantir que:

- todos os ativos criados, processados e excluídos sejam totalmente contabilizados;
- O acesso ao ativo de Informação da empresa é auditável para identificar data, hora, atividade e pessoa responsável;
- Indivíduos responsáveis são rastreáveis e podem ser responsabilizados.

xii. A trilha de auditoria deve ser protegida em termos de integridade e o período de retenção deve ser definido. Não deve conter dados sensíveis;

xiii. Restringir o acesso e a leitura dos arquivos de logs aos usuários autorizados;

xiv. Não registrar nos arquivos de log dados confidenciais utilizados na autenticação das credenciais de acesso (senhas, chaves privadas etc.) ou na autorização dos acessos (identificações ou senhas de sessão etc.);

xv. Permitir, com o mecanismo de geração de trilhas de auditoria, a configuração de mecanismo de coleta de logs externo ou centralizado;

xvi. Armazenar os arquivos de log de forma segura e possuir restrição de acesso, principalmente nos casos de permissão de alteração e exclusão;

xvii. Registrar, pelo menos, os seguintes eventos, quando aplicáveis:

- acesso ao ativo de informação da empresa, 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;
- falhas que ocorreram de criptografia.

xix. 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.

xx. Garantir que as entradas de log que incluem dados não confiáveis não sejam executadas como um código na interface de visualização de logs;

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

4.3.2. Identidade do Site / Aplicativo

i. Todo o domínio utilizado para objeto de cumprimento do contrato deve ser registrado no Brasil (Registro.BR), por exemplo: ".com.br";

ii. Em todas as suas peças de comunicação, o fornecedor deve usar o logotipo da Empresa disponível no link https://mondrian.claro.com.br/brands/nosvg/assinatura-claro.png. Esta aplicação deve seguir as orientações do Livro da Marca, desenvolvido pela área de Marketing da Claro.

   a) Deixar visível no menu e rodapé que o site pertence ao grupo de fornecedor;

   b) Exibir o nome do fornecedor;

   c) Disponibilizar link com direcionamento para o site institucional do fornecedor;

   d) Aplicar no site/aplicativo a submarca CLARO EMPRESAS (que se encontra disponibilizada no link https://mondrian.claro.com.br/brands/horizontal/default/claro-empresas.svg, quando o produto/serviço comercializado for relacionado à CLARO EMPRESAS, bem como seguir as orientações do Livro da Marca;

   e) Aplicar o selo https://mondrian.claro.com.br/brands/horizontal/default/agente-autorizado-claro-empresas.svg quando o produto/serviço for relacionado a um Agente Autorizado CLARO EMPRESAS, bem como também seguir regramentos do Livro da Marca;

iii. Quando for um aplicativo/site comercializado como CLARO:

   a) Utilizar os componentes padronizados do Design System da Claro (Mondrian) disponíveis no link https://mondrian.claro.com.br/snippets;

   b) Solicitar acesso para usar o Mondrian, por meio do formulário disponível no site no endereço https://mondrian.claro.com.br/suporte;

   c) Utilizar apontamento direto (não fazer download) ao links fornecidos nas bibliotecas de suporte do Mondrian Libraries (https://mondrian.claro.com.br/libraries) para uso de marcas Claro, marcas de produtos, logos de canais de TV, iconografia e fontes oficiais Claro e Embratel;

   d) Declarar na descrição da loja de aplicativos que é fornecedor Claro.

iv. É preferencial que o fornecedor responsável pelo site contrate a hospedagem na infraestrutura Cloud da Claro / Embratel;

v. No caso de site de fornecedores, o DNS do domínio do site deve, obrigatoriamente, apontar para os IPs fornecidos pela Claro (IP da CDN);

vi. Para sites próprios da Empresa e de fornecedores:

   1. **Domínios:**

      Todos os domínios registrados para as aplicações ou sistemas devem ter as contas administrativa, técnica e de cobrança gerenciadas pela Claro, e estarem associados aos names servers oficiais da Claro quando:

      a. Contiverem alguma marca registrada do grupo, incluindo Claro, Embratel, Net e Claro NXT;

      b. Forem para sites ou sistemas desenvolvidos especificamente para a Empresa;

      c. Estiverem hospedados em infraestrutura mantida pela Empresa;

d. Hospedarem páginas com identidade visual ou logomarca da Empresa ou grupo.

Nota: Alguns cenários podem estar isentos destas limitações, principalmente alguns recursos Cloud/SaaS, e devem ser avaliados pela Gerência de Segurança da Informação.

2. Governança Digital:

a. Para Site: Todo código do site deve ser armazenado no space gitlab fornecido pela Empresa. O código só entra em produção a partir deste gitlab, utilizando esteiras de Deploy Jenkins automatizadas da Empresa;

b. Para Apps: quando o código for de propriedade da Empresa, o código do app deve ser armazenado no space gitlab fornecido pela Empresa. O código só entra em produção a partir deste gitlab, utilizando esteiras de Deploy Jenkins automatizadas da Empresa;

c. Para as Bibliotecas Javascript de terceiros, sejam OpenSource ou licenciadas, devem ser adicionados os links para o código fonte original da versão utilizada (sem minificação). Caso o código fonte não possa ser disponibilizado por motivos de propriedade intelectual, deve ser fornecida documentação oficial atestando a aderência da Biblioteca JavaScript às leis de proteção de dados (LGPD ou GDPR ou equivalente). As bibliotecas e/ou documentação devem ser encaminhadas à Gerência de Segurança da Informação;

d. Para apps desenvolvidos por fornecedores, estes devem garantir que são disponibilizados somente nas apps stores pertencentes à Empresa, Android e Apple;

e. Todo Workload Cloud para sites e/ou apps devem rodar em conta cloud do CCOE (Cloud Center of Excelence) e usar a esteira de deploy do CCOE, pois esta já possui steps de segurança que garantem um deploy confiável do código;

f. O site do fornecedor deve gerar logs de todas as ações dos usuários que devem ser armazenadas em infraestrutura fornecida pela Empresa. Tal obrigatoriedade não se aplica no caso de apps;

g. Todo fornecedor deve utilizar o Tracking ID do Google Analytics fornecido pela Empresa. A ferramenta é implementada pela equipe de COE Digital. Como requisito para esta implementação, é necessário que o fornecedor libere o acesso ao seu Google Analytics;

h. Todos os relatórios de audiência podem ser acessados pelos integrantes da área de Analytics da Empresa;

Sempre que o usuário registrar um CPF no site do fornecedor, é necessário que o backend do site do fornecedor chame a API para geração do ClaroID que deve ser armazenado na variável do GA determinada. Para isso, deve ser enviado e-mail à Empresa através da caixa postal governanca.apps@claro.com.br,
O fornecedor deve apresentar à equipe de COE Digital – Tecnologia as seguintes informações (via caixa postal governanca.apps@claro.com.br):

i. O fornecedor deve apresentar à equipe de COE Digital – Tecnologia as seguintes informações (via caixa postal governanca.apps@claro.com.br):

- Lista de todas as tecnologias utilizadas para a construção do Frontend e do Backend/BFF que suporta o site ou app;
- Diagramas de arquitetura e de sequência do Frontend e do Backend/BFF;
- Listar os links dos repositórios oficiais onde estão armazenadas as versões utilizadas de todas as dependências de Bibliotecas Javascript utilizadas no Frontend bem como suas funções;
- Listar todos os endpoints das APIs que são chamadas pelo código-fonte, seja este desenvolvido pela Empresa ou terceiro ou por uma das bibliotecas da lista de dependências, bem como incluir a documentação dos recursos (swagger) chamados destas APIs;
- Armazenar todo código fonte do Frontend e do Backend/BFF nos repositórios de código da Claro (GitLab) e apresentá-lo caso seja solicitado pela Gerência de Segurança da Informação quando da análise do projeto.

4.3.3. Utilização de E-Mail ou E-Mail Marketing

i. Toda comunicação com o cliente utilizando correio eletrônico deve ser feita utilizando domínios corporativos. Não está autorizada comunicação através de domínios públicos (ex: Gmail);

ii. Para uso do e-mail marketing destinado a clientes, a CONTRATADA deve observar que:

a) O envio do e-mail deve conter a identificação do remetente, assunto e logotipo da CONTRATADA;

b) Na mensagem de e-mail, deve ser inserido um termo de responsabilidade, que alerte sobre as boas práticas de segurança na prevenção contra falsos e-mails que visam fraudar o destinatário (phishing);

c) Somente podem ser enviadas mensagens pelo endereço eletrônico vinculado ao seu domínio do fornecedor.

d) É vetada a prática do primeiro envio para se obter a permissão do destinatário para envios posteriores, que caracteriza a prática de SPAM;

e) Os clientes devem autorizar previamente o recebimento das mensagens (opt-in);

f) Para o envio de arquivos anexos, deve ser obtida autorização prévia e comprovável do destinatário, específica para o tipo de arquivo em questão;

g) A veiculação deve ser apenas de conteúdo no HTML ou TXT sem qualquer recurso que possa ocultar, disfarçar ou obscurecer de qualquer maneira o código original da mensagem;

h) Deve ser verificado se o código HTML está de acordo com as recomendações do W3C utilizando, por exemplo, o validador disponível no site http://validator.w3.org/. Algumas aplicações antispam incluem a validação do código em seus testes e podem até atribuir pontuação à mensagem, caso o código não seja válido;

i) Se o e-mail estiver em formato HTML, deve-se oferecer em local visível a possibilidade de visualizar o mesmo conteúdo em uma página da web, já que alguns softwares podem

bloquear ou mesmo impedir a correta visualização. Componentes da mensagem, tais como imagens, hiperlinks, endereços eletrônicos, áudios e vídeos devem ser hospedados em servidores pertencentes à Empresa;

j) É vetada a utilização de link externo no corpo do e-mail;

k) É vedado o envio de arquivos com autoexecutáveis;

l) Deve-se limitar o tamanho das mensagens em 40MB (cabeçalho+texto+anexo) a fim de não sobrecarregar o sistema de envio nem a caixa de entrada do destinatário;

m) O conteúdo da mensagem deve ser genérico e ter como característica a impessoalidade, ou seja, não deve conter dados cadastrais de clientes da Empresa.

4.3.4. 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 de forma on-line pelo **período mínimo de 5 (cinco) anos;**

ii. 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;**

iii. 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;

iv. 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.

4.4. Proteção de Dados

i. As informações e dados de clientes, prospects etc. devem ser classificadas conforme critérios abaixo e criptografadas no armazenamento e transporte;

- **CONFIDENCIAL***:* Informação de alto impacto deve ser protegida por:

  a) sua relevância sobre decisões estratégicas, impacto financeiro, oportunidades de negócio, potencial de fraude ou requisitos legais;

  b) seu impacto nos interesses do negócio, de seus clientes, fornecedores e colaboradores.

  São informações que devem circular apenas entre os colaboradores definidos pelo executivo responsável pela geração da informação.

- **CONFIDENCIAL LGPD**: Informação de alto impacto com dados de pessoa natural, que deve ser protegida por:

  a) sua relevância para fins de atendimento à Lei Geral de Proteção de Dados Pessoais, podendo ser de cliente, colaborador próprio, terceiros ou prestadores de serviço;

  b) seu impacto nos interesses do negócio, de seus clientes, fornecedores e colaboradores.

- **USO INTERNO:** Informação que, sem reserva ou restrição, deve ser mantida no âmbito interno da empresa e não deve ser divulgada ou ser disponível externamente. O acordo de

confidencialidade deve estar previsto no contrato da contratada e deve ser assinado entre a contratada e seus recursos.

- **PÚBLICA**: Informação cuja divulgação não afeta à empresa em termos de perda de imagem e/ou econômica/financeira

ii. As operações de criptografia e descriptografia dos dados devem ser realizadas apenas em servidores seguros em ambiente seguro;

iii. As chaves de criptografia devem ser individuais e somente o dono da chave deve ter acesso a ela. O fornecedor deve possuir uma chave de criptografia exclusiva para troca de arquivos de produção e, caso o fornecedor possua mais de uma sede, as chaves de criptografia devem ser diferentes;

iv. A proteção, bem como o termo de consentimento de uso de dados pessoais e dados pessoais sensíveis devem estar de acordo com à LGPD.

4.5. 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.

4.6. 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 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.

4.7. Segurança nas Aplicações/Aplicativos Móveis

i. Qualquer sistema desenvolvido para plataformas móveis, como Android, iPhone, iPad, Symbian etc., deve obrigatoriamente cumprir com os requisitos abaixo com o objetivo de evitar a exploração de vulnerabilidades comuns em aplicativos destas plataformas, que possuem características únicas em relação a sistemas desktops e aplicações web;

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

A) 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 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 logs do aplicativo não devem armazenar dados sensíveis no dispositivo;

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

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

j) 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.);

k) O aplicativo deve utilizar as mínimas permissões necessárias para seu funcionamento para garantir a privacidade dos usuários e a usabilidade do sistema;

l) 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;

m) 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;

n) 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;

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

p) 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;

q) 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;

r) 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;

s) 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;

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

u) 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;

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

B) Gerenciamento de Sessão

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

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

b) O aplicativo deve possuir a funcionalidade de bloqueio de tela por tempo de inatividade (timeout).

- Essa funcionalidade de bloqueio deve ser implementada com um código numérico PIN (com um mínimo de 4 dígitos) ou com um padrão de desenho na tela para assegurar que o aplicativo não seja utilizado de forma indevida devido à inatividade do dispositivo;
- A aplicação deve permitir configurar o tempo de expiração e o código ou padrão utilizado.

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

C) Proteção de Dados

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

b) O aplicativo deve utilizar SSL 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), inclusive 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 autocompletar 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.

4.8. Incidentes de Segurança e Privacidade

i. Para garantir a execução da continuidade do negócio, bem como cumprimento da Lei Geral de Proteção de Dados (LGPD), em caso de qualquer acesso não autorizado, divulgação indevida, exposição indesejada e/ou situação acidental ou intencional de destruição, deleção, perda, alteração ("incidentes de segurança"), a CONTRATADA deve seguir os seguintes passos:

a) Notificar imediatamente à caixa postal CSIRT@claro.com.br sobre a ocorrência de incidentes, irregularidades ou eventos suspeitos que afetem ou possam afetar a marca, imagem da Empresa, devendo conter, no mínimo, as seguintes informações:

(i) data e hora do incidente;

(ii) data e hora da ciência;

(iii) relação dos tipos de dados afetados pelo incidente;

(iv) número de usuários afetados (volumetria do incidente;

(v) a informação quanto aos titulares dos dados afetados;

(vi) os riscos relacionados ao incidente;

(vii) as medidas que foram ou são adotadas para reverter ou mitigar os efeitos do incidente;

(viii) a indicação das medidas de segurança técnicas e administrativas utilizadas para a proteção dos dados;

(ix) os motivos da demora, no caso de a comunicação não ter ocorrido dentro do prazo de 24 (vinte e quatro) horas, sem prejuízo de incorrer nas penalidades contratuais por inadimplemento de seus termos;

(x) dados de contato do encarregado do fornecedor ou, não havendo encarregado, a outra pessoa junto à qual seja possível obter maiores informações sobre o ocorrido; e

(xi) descrição das possíveis consequências do evento;

b) Notificar imediatamente o responsável da Empresa pela contratação;

c) Garantir que os logs para análise ou perícia estejam disponíveis quando solicitados pela Empresa;

d) Auxiliar e/ou implementar medidas de correção de vulnerabilidades, mitigação de riscos e/ou danos.

4.9. 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 da Claro, contendo autoavaliação (selfassessment) 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 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.

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;
- 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. 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.

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 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.