Segurança da Informação e Proteção de Dados

para fornecedores CPQD.

ANEXO - SEGURANÇA DIGITAL

Sumário

1. Das políticas, normas e procedimentos de cibersegurança e garantia de segurança de dados e/ou informações

1.1. A CONTRATADA garante possuir e cumprir a segurança das informações em seu ambiente, em um modelo sustentável de gerenciamento de Segurança Digital com a aplicação de políticas e normas, assegurando a integridade, a confidencialidade, a disponibilidade e segurança, das informações e dos seus respectivos sistemas, tanto física quanto logicamente, implementando todas as medidas técnicas, processuais e/ou organizacionais para o cumprimento deste Anexo de segurança. A CONTRATADA também é responsável pelo cumprimento das regras de segurança do CPQD quando a CONTRATADA acessa as informações e os sistemas do CPQD (incluindo, quando aplicável, o software utilizado pela CONTRATANTE, o qual a CONTRATADA desenvolveu).

1.2. Durante o acesso às informações ou aos sistemas em ambientes da CONTRATANTE, inclusive no exercício do papel de desenvolvedora, a CONTRATADA se responsabiliza também pelo cumprimento integral das regras de segurança da CONTRATANTE.

1.2.1. Eventuais custos relacionados à manutenção do sistema de gestão e de controles de segurança da informação e proteção de dados, incluindo, quando aplicável, a recuperação de informações, sistemas ou infraestruturas, serão de total responsabilidade da CONTRATADA.

2. Privacidade, proteção de dados e segurança da informação

2.1 Todos os bancos de dados e/ou informações de propriedade da CONTRATANTE, aos quais a CONTRATADA tiver acesso no exercício das suas obrigações, são estritamente confidenciais e, portanto, somente poderão ser utilizados em observância à *finalidade* do cumprimento do presente Contrato.

a - a propriedade, restrição e finalidade acima descritas, a CONTRATADA assegura, em nenhuma circunstância, utilizar dados e/ou informações da CONTRATANTE para benefício próprio e/ou de terceiros.

2.2 A CONTRATADA, quando controladora ou operadora de dados, se compromete em cooperar com a CONTRATANTE para responder às eventuais solicitações que tenham por objetivo o exercício dos direitos dos titulares de dados, especificados na legislação vigente de Proteção de Dados, dentre eles os que se referem, entre outros, à *transparência*, à *informação*, ao *acesso*, à *retificação*, à *exclusão (direito ao esquecimento),* à *limitação* e/ou à *oposição ao tratamento*, bem como a possibilidade de *portabilidade* de seus dados e/ou suas informações.

2.3 A CONTRATADA garante que não compartilhará nem de outra forma divulgará os dados e/ou informações da CONTRATANTE e, tampouco, permitirá o tratamento destes por seus representantes, subcontratados e/ou terceiros.

2.4 Caso exista a necessidade de a CONTRATADA *transferir*, *compartilhar*, *divulgar* e/ou *permitir o tratamento* de dados da CONTRATANTE por terceiros, deverá, prévia e formalmente, notificar a CONTRATANTE para que esta conceda sua anuência.

2.5 As informações e/ou dados de propriedade da CONTRATANTE devem estar classificados e rotulados, com medidas de proteção aplicadas em todo o ciclo de vida da informação, isto é, desde a criação/coleta até a eliminação pela CONTRATADA *(custodiante da informação)*, seguindo as premissas abaixo:

2.5.1 Criação ou coleta de dados/informações:

2.5.1.1 A CONTRADA se compromete, para fins de classificação e rotulação das informações, a seguir as recomendações enumeradas abaixo:

a- SECRETA: informação de alta sensibilidade que deve ser protegida por sua relevância; versa sobre decisões estratégicas, impacto financeiro, oportunidades e/ou segredo comercial, potencial de fraude, requisitos contratuais e/ou legais.
b- CONFIDENCIAL: informação sigilosa, interna para áreas e/ou projetos cujo acesso deve ser controlado e restrito a um grupo reduzido de pessoas, devendo ser protegida por seu impacto nos interesses do negócio, de seus clientes ou associados e colaboradores.
c- RESERVADA: informação que, sem reserva ou restrição, deve ser mantida no âmbito interno do Contrato e não deve ser divulgada ou colocada à disposição externamente.

2.5.2 Armazenamento de dados/informações:

2.5.2.1 As informações e/ou dados da CONTRATANTE devem ser armazenados em diretórios/bancos de dados exclusivos e segregados, seguindo todas as regras determinadas neste anexo.

a- O armazenamento em nuvem está autorizado somente mediante aprovação expressa da CONTRATANTE, para todas as infraestruturas do escopo do Contrato, independentemente da *Classificação da informação*.
b- Dados e/ou informações classificados como secretos ou confidenciais devem ser armazenados com criptografia.

2.5.3 Processamento dos dados/informações:

2.5.3.1 A CONTRATADA se compromete a contar, em todo tipo de processamento de dados e/ou informações decorrentes do objeto do presente Contrato, com medidas técnicas, processuais e organizacionais seguras, sendo configuradas de maneira a robustecer e garantir a segurança de tais dados, de acordo com todos os requisitos contidos neste anexo.

2.5.4 Transferência de dados/informações:

2.5.4.1 A CONTRATADA assume que em qualquer modalidade de comunicação, integração e/ou transferência de dados e/ou informações, haverá a aplicação da metodologia Triple A *(Authentication, Authorization and Accounting)*, além da utilização de técnicas de criptografia, anonimização/mascaramento dos dados e/ou quaisquer outras medidas de segurança que se fizerem necessárias para garantir a segurança e proteção dos dados e informações durante a eventual transferência, sem dispensar ainda a anuência prévia, conforme já disposto no *item 2.4* deste anexo.

2.5.5 Eliminação dos dados/informações:

2.5.4.1 A CONTRATADA se compromete que, quando do término do presente Contrato, ou ainda, em cumprimento de solicitação feita pela CONTRATANTE, todos e quaisquer dados e/ou informações de propriedade da CONTRATANTE obtidos, processados, armazenados e/ou transmitidos para a execução do objeto deste Contrato, serão completamente destruídos com uso de medidas técnicas, processuais e organizacionais que visem garantir a eliminação segura e a impossibilidade de restauração.

2.5.4.2 As mídias óticas e/ou eletrônicas, tanto as fixas como as removíveis, que contenham dados e/ou informações da CONTRATANTE, quando não forem mais utilizadas, requerem os seguintes cuidados no descarte, os quais a CONTRATADA assume observar e cumprir:

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, devem ser prestados por fornecedor com experiência comprovada e controles de segurança adequados.

2.6 Rescisão do Contrato: proteção de dados/informações

2.6.1 Quando da rescisão do presente Contrato ou mediante solicitação por escrito da CONTRATANTE, o que ocorrer primeiro, a CONTRATADA cessará imediatamente e garantirá que seus subcontratados, quando houver, cessem imediatamente, todo e qualquer uso de dados e/ou informações da CONTRATANTE, devolvendo-os, eliminando-os, destruindo-os ou tornando-os anônimos de forma permanente, a depender do pedido da CONTRATANTE, utilizando para tanto, em cada caso, as medidas de segurança aplicáveis e necessárias, sejam elas técnicas, processuais e/ou organizacionais.

a- Se a legislação vigente e aplicável não permitir que a CONTRATADA destrua ou elimine os dados e/ou informações da CONTRATANTE, a CONTRATADA declara que não usará esses dados e/ou informações para nenhuma outra finalidade que não seja a que se encontra na obrigação legal ou regulatória e nos Contratos aplicáveis, bem como que manifestará por escrito à CONTRATANTE tal impossibilidade assim que tomar ciência.

2.6.2 As empresas terceiras, parceiras ou subcontratadas da CONTRATADA, que foram expressamente autorizadas a utilizar os dados e/ou informações da CONTRATANTE em cumprimento do objeto deste Contrato, devem respeitar as cláusulas definidas neste *Anexo de segurança*, assumindo, por meio deste, a CONTRATADA tal responsabilidade de se fazer cumprir.

3. Requisitos de segurança digital

3.1. A CONTRATADA deve seguir padrões de segurança e arquiteturas de referência adequadas de acordo com os requisitos de Segurança Digital colocados à disposição pela CONTRATANTE para todos os sistemas e/ou aplicativos próprios que serão desenvolvidos para cumprimento do objeto deste Contrato, que manipulem dados ou informações da CONTRATANTE, com o objetivo de garantir os seguintes princípios: confidencialidade, integridade e disponibilidade. O objetivo é apresentar os padrões e premissas arquitetônicas para o desenvolvimento e a manutenção seguros de sistemas que manipulem, transmitam ou armazenem informações da CONTRATANTE.
3.2. Caso seja necessário o desenvolvimento ou a aquisição de novas soluções ou, ainda, utilizar soluções da CONTRATADA, esta mesma deverá solicitar à CONTRATANTE, via seu gestor de Contrato a análise de riscos à Segurança Digital para aprovação prévia. A solução somente deverá ser utilizada em produção após a aprovação da CONTRATANTE.
3.3. A CONTRATADA deverá conhecer e cumprir os requisitos estabelecidos nos documentos anexos no item 3.5 deste documento.
3.4. Todos os entregáveis, incluindo o desenvolvimento, produzido para e/ou fornecido para a CONTRATANTE como parte dos serviços efetuados pela CONTRATADA ou qualquer subcontratado da CONTRATADA que estão cobertos sobre a lei de direitos de propriedade intelectual (direito de propriedade industrial, literário e artístico) devem, em respeito ao código de propriedade intelectual brasileiro, serem atribuídos exclusivamente à CONTRATANTE.
3.5. A CONTRATADA deverá garantir a conformidade, quando aplicável, com as seguintes melhores práticas de mercado:
OWASP Application Security Verification Standard (ASVS)
CIS Controls
Cloud Security Alliance CCM
ABNT NBR ISO/IEC 27001:2022

4. Gestão de incidentes de segurança

4.1. A CONTRATADA notificará prontamente por meio do canal de denúncias Security CPQD (security@cpqd.com.br) a CONTRATANTE sobre qualquer fato que comprometa a segurança da informação, tanto física quanto logicamente (por exemplo, tentativas de invasão, roubo e vazamento de informações, novas vulnerabilidades e incidentes de segurança da informação) e tomará todas as medidas necessárias para corrigir a situação e manter a segurança de todas as informações da CONTRATANTE, durante e após a vigência do Contrato.
4.1.1. A notificação à CONTRATANTE comunicando a ocorrência do incidente deverá ser imediata, ou seja, logo após a tomada de conhecimento.
4.2. A CONTRATADA deve garantir que os *logs* para análise ou perícia estejam disponíveis quando solicitados pela CONTRATANTE.

5. Controles de auditoria e revisão de atividades de sistemas de informação

5.1. A CONTRATANTE poderá anualmente, por si própria ou usando um serviço terceirizado, realizar a auditoria e/ou *assessment* (avaliação) de segurança a fim de garantir que o prestador de serviços esteja cumprindo suas obrigações, mantendo o sistema de gestão de segurança e/ou garantindo a segurança da infraestrutura, mas também para responder a qualquer pedido feito por uma autoridade judicial ou administrativa.
5.2. As avaliações podem ser realizadas presencialmente, caso seja apropriado, e as visitas serão previamente agendadas.
5.3. Caso o relatório da avaliação revele uma quebra significativa das obrigações da CONTRATADA na prestação dos serviços do presente Contrato, a CONTRATADA será informada via emissão do relatório e deverá implementar todas as medidas corretivas necessárias, sem qualquer custo para a CONTRATANTE, no prazo de trinta (30) dias a partir da data em que o descumprimento for informado pela CONTRATANTE.
5.4. Durante o período de avaliação ou auditoria, os níveis acordados de serviço não poderão ser alterados.
5.5. Será necessário também que a CONTRATADA realize um teste de invasão no ambiente e serviço em escopo do fornecimento da CONTRATANTE e os resultados e planos de correção devem ser compartilhados com a CONTRATANTE.
5.6. Quando for necessário, a CONTRATANTE deverá ter acesso a registros e *logs* que identifiquem todas as ações realizadas pelos colaboradores da CONTRATADA de forma que seja possível identificar qual foi o operador e suas respectivas ações indicando a data e hora e qual equipamento foi utilizado.
5.6.1. Os arquivos, registros e *logs* devem ser armazenados de forma segura e possuir restrição de acesso, principalmente nos casos de permissão de alteração ou exclusão. O acesso à leitura dos arquivos, registros e *logs* deve ser restrito aos usuários autorizados seguindo as orientações previstas em “Controle de acesso e gerenciamento de identidade”.
5.7. A CONTRATANTE também poderá realizar avaliações técnicas, mediante agendamento com a CONTRATADA. Os testes serão realizados apenas no escopo do serviço prestado. Caso sejam identificados pontos de correção, a CONTRATADA deve seguir o prazo abaixo para correção:

Tipo de vulnerabilidade	Prazo esperado para a correção
Crítico	5 dias
Alto	8 dias
Moderado	30 dias
Médio	60 dias
Leve	90 dias

6. Controle de acesso e gerenciamento de identidade

6.1. Para sistemas em que a CONTRATANTE fornecerá acesso à CONTRATADA, as regras serão as mesmas utilizadas nas políticas vigentes para a CONTRATANTE. Para sistemas que a própria CONTRATADA faz a gestão de acessos, deverão ser implantados os controles de acessos que garantam não repúdio dos acessos e *logs* para investigação posterior, caso solicitado pela CONTRATANTE.
6.2. As regras de controle de acesso devem respeitar revisões periódicas de acessos e perfis, senhas complexas, revogação de acesso e *logs*. Não deve existir nenhum processo ou função que altere ou apague qualquer registro da trilha de auditoria, salvo o *script* de retenção. Os registros de auditoria devem ser armazenados por no mínimo 90 dias (on-line) e devem suportar o prazo de retenção padrão definido pela legislação atual.
6.3. Caso a CONTRATADA tenha acesso a dados críticos sensíveis, como, por exemplo, dados de sigilo telefônico ou dados sensíveis de pessoas físicas, a CONTRATANTE se reserva o direito de exigir medidas adicionais de segurança para colaboradores e computadores e a CONTRATADA não deverá realizar consultas de forma massiva. As medidas incluem, entre outras:
6.3.1. Treinamentos de segurança digital para os colaboradores;
6.3.2. Bloqueio do acesso à internet e restrições nas máquinas, liberando somente as ferramentas corporativas essenciais para execução das atividades;
6.3.3. Ferramentas de monitoramento.
6.4. A CONTRATADA deve seguir todos os controles referentes à gestão de acessos lógicos, conforme determinado pela CONTRATANTE, tais como:
6.5. Gestão do ciclo de vida dos acessos lógicos
6.5.1. Acessos lógicos são os acessos a sistemas, software e ambientes da CONTRATANTE. Acessos lógicos envolvem as credenciais de acesso (usuário, senha e autenticação de dois fatores, caso aplicável), que permitem acesso pelos contratados aos sistemas da CONTRATANTE.
6.5.2. A CONTRATADA deverá conhecer e cumprir os requisitos descritos nos procedimentos estabelecidos na política de controle de acesso lógico da CONTRATANTE.
6.5.3. A CONTRATADA é responsável pelo ciclo de vida dos usuários (cadastro, atualização, revisão, férias, afastamento e desligamentos) pela acuracidade dos dados cadastrais fornecidos à CONTRATANTE. O gestor da área CONTRATANTE é responsável pela validação e acompanhamento contínuos dos cadastros gerados pela CONTRATADA, assim como pela manutenção e inativação dos registros, conforme normativa interna.
6.5.4. A CONTRATADA deve realizar o desligamento imediato colaboradores que estejam ausentes nas operações da CONTRATANTE devido a licença, afastamento ou férias por mais de 30 dias, bem como, realizar as transferências de área, cargo e de qualquer atualização que se fizer necessária de todo e qualquer cadastro de usuário que possua acesso a sistemas da CONTRATANTE, com suas devidas revisões e revogações de acesso quando aplicáveis em decorrência dessa movimentação. Tal procedimento se faz necessário por razões de segurança dos dados.
6.5.5. A CONTRATADA deve responder às revisões das certificações sempre que solicitado pela CONTRATANTE. Apenas os acessos necessários para a função atual do colaborador devem permanecer liberados. Não é permitido delegar esta atividade para outro colaborador que não tenha a função de gestão de usuários.
6.5.6. Cumprir o prazo de até 1 (um) dia útil para comunicar todas as ações do ciclo de vida dos usuários, conforme citado acima.
6.6. Uso das senhas e credenciais de acessos

No que tange ao uso das senhas, a CONTRATADA deve cumprir os requisitos abaixo:

6.6.1. As senhas são pessoais e intransferíveis, portanto, não devem ser compartilhadas.
6.6.2. Nenhum colaborador, quer seja da CONTRATANTE ou da CONTRATADA, tem autorização para alterar a senha das credenciais de acesso antes do envio para os seus responsáveis.
6.6.3. Apenas o responsável pela credencial de acesso pode determinar e fazer uso do usuário e da senha das credenciais de acesso, ou seja, a senha deve ser cadastrada pelo próprio colaborador, NÃO podendo ter nenhuma interferência de outros colaboradores ou compartilhamento.
6.6.4. O solicitante responsável pela requisição de acessos lógicos NÃO tem autorização para trocar as senhas antes do envio para os seus responsáveis.
6.6.5. Os gestores NÃO têm autorização para trocar as senhas antes do envio para os seus responsáveis.
6.6.6. Os colaboradores devem receber as senhas expiradas para que realizem a troca. Não devem ser aceitas senhas não expiradas ou previamente definidas que não sejam passíveis de alteração.
6.6.7. Na definição das senhas não devem ser usadas senhas fracas, senhas-padrão ou com combinações óbvias. O CPQD determina os critérios de qualidade das senhas e informará/reforçará esses critérios no momento da definição da senha.
6.6.8. Devem ser utilizadas senhas complexas com pelo menos 10 caracteres, incluindo números, letras maiúsculas e minúsculas e caracteres especiais.
6.6.9. Cada colaborador é responsável pelas ações realizadas com o seu par usuário e senha, o que o torna pessoal e intransferível.
6.6.10. Contas privilegiadas de serviço, genéricas e RPA (Robotic Process Automation) devem impreterivelmente estar dentro do cofre de senhas definido pelo CONTRATANTE, com o processo de controle de senhas e monitoramento das contas.

7. Gerenciamento de ativos e configuração de sistemas

7.1. A utilização ou integração de robô (RPA – Robotic Process Automation) com sistemas da CONTRATANTE ou outras formas de integrações entre sistemas e banco de dados de forma automatizada (APIs, integradores, consultas a banco de dados, etc.) deverão ser submetidas à avaliação e à aprovação da CONTRATANTE, especialmente em relação a qualquer necessidade de integração a interfaces, sistemas, aplicativos, bancos de dados e serviços, etc. Somente após a aprovação prévia da CONTRATANTE a integração deverá ocorrer. Para a avaliação será necessária a criação de um desenho da arquitetura da solução.
7.2. Todos os processos e projetos de automação aprovados pelas áreas destacadas acima deverão seguir as diretrizes preestabelecidas conforme especificado pela CONTRATANTE, se aplicável.
7.3. A CONTRATADA deverá se responsabilizar pelo uso seguro de todos os ativos que transferem dados da CONTRATANTE, quer os ativos sejam fornecidos pela CONTRATANTE ou não. Ativos lógicos também devem ser incluídos no mesmo padrão de segurança, incluindo e-mails, domínios, marcas e demais ativos lógicos utilizados no exercício deste Contrato.
7.4. Os recursos da CONTRATADA que irão realizar atividades objeto deste Contrato, em instalações/prédios administrativos da CONTRATANTE, somente poderão se conectar ao nosso ambiente corporativo após seus equipamentos (dispositivos móveis, computadores, etc.) serem autorizados pelas áreas técnicas responsáveis da CONTRATANTE e deverão estar com aplicação de *hardening* para controle de violação de dados.
7.5. Gestão de *logs*
7.5.1. A CONTRATADA deve manter uma gestão de *logs*, os quais devem estar disponíveis mediante solicitação da CONTRATANTE.
7.5.2. Os ativos da CONTRATADA relacionados ao objeto deste Contrato devem prover *logs* que informem no mínimo:
- Login do usuário.
- Data.
- Hora.
- Tipo de evento.
- Endereço de IP e *Hostname* do equipamento.

7.6. Os arquivos de *log* devem ser armazenados de forma segura e possuir restrição de acesso, principalmente nos casos de permissão de alteração e exclusão. O acesso e a leitura aos arquivos de *logs* devem ser restritos aos usuários autorizados.
7.7. Não deve existir nenhum processo ou função que altere ou apague qualquer registro da trilha de auditoria, salvo o *script* de retenção.

8. Segurança de rede

8.1. A CONTRATADA deverá controlar os tratamentos realizados com dados pessoais e sensíveis quando utilizados ativos de propriedade da CONTRATANTE, por exemplo, equipamentos informáticos (ex.: notebooks), aplicativos, sistemas, ferramentas, servidores, bancos de dados, etc. Isso implica:
8.1.1. Monitorar desvios de acesso a dados pessoais e sensíveis, ou seja, identificar as pessoas não autorizadas (quando, quem e o que fez).
8.1.2. Poder controlar o que se pode fazer com a informação (leitura, cópia, impressão e modificação) de forma individualizada.
8.2. A CONTRATADA deve manter um procedimento de segurança lógica que englobe e documente os processos para:
8.2.1. Prover um segmento de rede exclusivo e segregado para os serviços contratados pela CONTRATANTE.
8.2.2. Controlar e restringir os acessos de outras redes para a rede exclusiva utilizada na prestação do serviço, por meio de regras restritivas de *firewall*.
8.2.3. Prover, quando solicitado pela CONTRATANTE, diagramas físicos e lógicos atualizados das redes que suportam as operações que são objeto deste CONTRATO, contendo os equipamentos utilizados e suas interconexões.
8.2.4. Implementar regras de controle de comunicação com a internet de acordo com a necessidade da operação.
8.2.5. Proteger as conexões de rede da empresa de outras redes externas, de acordo com as melhores práticas de segurança da informação.
8.2.6. Os ativos da CONTRATADA devem prover proteção contra códigos maliciosos, tais como antivírus e *personal firewall (*atualizados diariamente).
8.2.7. A instalação e utilização de pontos de acesso sem fio devem ser controladas e configuradas conforme as melhores práticas do mercado para padrões de segurança.

8.3. Os ativos envolvidos na prestação do serviço para a CONTRATANTE devem ser contemplados por um processo de *hardening*:
  8.3.1. Deve haver um método de *backup* das informações da CONTRATANTE, o qual deve ser testado periodicamente.
  8.3.2. A CONTRATADA deve restringir o acesso físico aos pontos de rede acessíveis publicamente, pontos sem fio, *gateways* e dispositivos portáteis.
  8.3.3. Os computadores devem ser bloqueados sempre que o seu usuário se ausentar ou por inatividade e devem ser desbloqueados com a senha de acesso do usuário.
  8.3.4. Os equipamentos envolvidos na operação devem possuir apenas conexões, interfaces, aplicativos e dispositivos necessários para a sua finalidade. A CONTRATADA deve bloquear a utilização de dispositivos que permitam a gravação de informações em mídias ou periféricos.

9. Gestão de ameaças e vulnerabilidades

9.1. A CONTRATADA deverá manter um processo de gestão de vulnerabilidade que abranja totalmente o escopo de serviços prestados para a CONTRATANTE, considerando identificação, classificação da vulnerabilidade, classificação do risco, plano de correção e registro de correção. O inventário de ativos como base para monitoramento de vulnerabilidades deverá estar completo e íntegro.
9.2. *Patches* deverão ser aplicados em janelas programadas a todos os ativos no inventário, cumprindo o prazo descrito no item 5.7 deste documento.
9.3. A CONTRATADA deve definir um procedimento para calcular o risco de cada vulnerabilidade identificada, considerando critérios de classificação da informação, probabilidade de exploração da vulnerabilidade e o impacto relacionado.
9.4. Os resultados também devem ficar disponíveis para consulta da CONTRATANTE.

10. Conscientização e treinamento de cibersegurança

10.1. A CONTRATADA deve manter um programa de conscientização periódico garantindo que seus colaboradores estejam treinados nos temas de segurança digital.

  10.1.1. A CONTRATANTE poderá solicitar a qualquer momento evidências do programa de conscientização da CONTRATADA. A CONTRATADA deverá apresentar a documentação em resposta à solicitação da CONTRATANTE no prazo de 30 dias corridos.
  10.1.2. Caso a CONTRATANTE identifique uma necessidade de melhoria no programa de conscientização da CONTRATADA, a CONTRATADA avaliará a sugestão e apresentará um plano de ação para atender à demanda ou uma formalização da impossibilidade de aplicação no prazo de 30 dias corridos.

11. Gestão de continuidade de negócios e gestão de crises

11.1. A CONTRATADA deverá implementar e manter um sistema de gestão de continuidade de negócios (SGCN) para garantir a disponibilidade e manutenção dos serviços/produtos prestados à CONTRATANTE, dentro dos prazos acordados, considerando:
- A CONTRATADA deverá fornecer, a qualquer momento, evidências da manutenção do SGCN (atualização dos documentos, planos e teste do período vigente do ciclo de GCN).
- A CONTRATADA deverá fornecer a qualquer momento, quando solicitado pela CONTRATANTE, as informações referentes à infraestrutura que suporta as atividades da CONTRATADA, bem como o mapeamento das localidades e o número de estações de atendimento disponíveis em cada uma das localidades onde estas são realizadas.
- A CONTRATADA deverá informar à CONTRATANTE toda e qualquer alteração em seu ambiente de trabalho e nos ambientes de contingência que estejam relacionados ao objeto ora contratado para o perfeito cumprimento desta cláusula.

11.2. Política de gestão de continuidade de negócios

A CONTRATADA deve publicar e divulgar a política de gestão de continuidade de negócios (GCN) a todos os seus funcionários que estejam relacionados ao objeto ora contratado, ficando sob sua responsabilidade o cumprimento das diretrizes.
Os custos relacionados à manutenção do sistema de gestão de continuidade de negócios, planos de contingência e de recuperação, serão de total responsabilidade da CONTRATADA.

11.3. Gestão de riscos para a continuidade de negócios
Deverá ser realizado um processo de gestão de riscos que possam afetar produtos e serviços contratados, com a identificação, a classificação e os planos de ação associados.

11.4. Planos de continuidade de negócios (PCN)

Os planos de continuidade de negócios deverão contemplar:

- Plano de continuidade operacional para os processos que estejam envolvidos nos produtos e/ou serviços fornecidos à CONTRATANTE.
- Plano de resposta de emergência para os incidentes com risco iminente à vida.
- Plano de gestão de incidentes com os canais e fluxo de comunicação ao CONTRATANTE.
- Plano de gestão de crises com os canais e fluxo de comunicação ao CONTRATANTE.
- Plano de recuperação de desastres para as infraestruturas críticas.

11.5. Plano de testes e validação
Todos os planos de continuidade de negócio deverão ser testados de 12 em 12 meses com coleta de evidências.
As evidências devem estar disponíveis para consulta da CONTRATANTE.

11.6. Estratégia de continuidade de negócios
Redundância e contingências para os recursos críticos para o fornecimento de serviços e/ou produtos nos prazos acordados:

- Água.
- Energia elétrica comercial.
- Comunicação (links, rede de comunicação, telefonia, e-mail, etc.).
- Local de trabalho (ou alternativa, por exemplo: teletrabalho).
- Infraestrutura tecnológica ou de produção.
- Sistemas e backup.
- Cadeia de abastecimento.
- Pessoas.
- Demais recursos críticos.

11.7. Processo de gestão de crises

Ter um processo formal de gestão de crises, com a definição de papéis e responsabilidades, matriz de crise, fluxo e plano de comunicação.
Qualquer evento que gere impacto para a CONTRATANTE (exemplo: interrupção, exposição da marca, pandemia) deverá ser comunicado nos canais definidos nos planos.

11.8. Plano de conscientização e treinamento para continuidade de negócios
As equipes deverão ser treinadas e conscientizadas sobre o tema de GCN e os planos em que atuam a cada 12 meses.

11.9. Volta à normalidade

Devem ser desenvolvidos e implantados procedimentos de volta à normalidade após um incidente, utilizando-se dos planos de respostas específicos para cada tipo de cenário avaliado após a realização da análise de riscos.

11.10. Melhoria contínua do sistema de gestão de continuidade de negócios

Em todas as etapas do SGCN devem ser observadas as melhorias e as lições aprendidas para implementação.

12. Segurança física e ambiental

12.1. Para as operações localizadas em instalações de propriedade da CONTRATADA, esta deve:

12.1.1. Caso solicitado pela CONTRATANTE, colocar à disposição um ambiente logicamente reservado com controles de segurança físicos e/ou eletrônicos que garantam acesso individual e controlado. As informações de controle de acesso devem ser colocadas à disposição no prazo de até 24 horas a partir da solicitação, com um armazenamento disponível por no mínimo 60 meses ou a duração do Contrato, prevalecendo o maior, quando solicitado pela CONTRATANTE. O objetivo é esclarecer incidentes relacionados ao ambiente físico e oferecer respaldo para fins de auditorias que se façam necessárias.

12.1.2. Manter as portas e janelas fechadas quando não utilizadas e dotadas de proteções externas, principalmente quando estiverem localizadas no andar térreo.

12.1.3. Instalar sensor de presença, para inibir o acesso por qualquer porta e janela acessível. As áreas desocupadas devem possuir um sistema de alarme que permaneça sempre ativado.

12.1.4. Monitorar rigorosamente o ambiente interno por CFTV, de forma que seja possível visualizar todas as PAs (independente do mobiliário existente) e acessos.

12.1.5. Monitorar rigorosamente por CFTV e alarmes os acessos de emergência e outros possíveis acessos (ex.: janelas).

12.1.6. Prover armazenamento das imagens gravadas pelo sistema de CFTV por, no mínimo, 120 (cento e vinte) dias e colocá-las à disposição em até 24 (vinte e quatro) horas, quando solicitado pela CONTRATANTE e se certificando de que as imagens possuam qualidade suficiente para identificar ações suspeitas. O objetivo é esclarecer incidentes relacionados ao ambiente físico.

12.1.7. Assegurar que as mídias de armazenamento das gravações de voz e das imagens sejam armazenadas em locais seguros.

12.1.8. As informações de clientes da CONTRATANTE não devem ser armazenadas pela CONTRATADA, com exceção das gravações de atendimento e de processos previamente acordados entre as Partes.

12.1.9. Prover acesso às imagens de CFTV, em tempo real, para monitoramento pela CONTRATANTE.

12.1.10. Atender às normas e leis reguladoras de segurança, detecção e combate a incêndio (sistema de segurança, brigada de incêndio, bombeiro civil residente, etc.).

12.1.11. Apresentar Auto de Vistoria do Corpo de Bombeiros (AVCB), ou seu congênere para as instalações, com a devida aprovação para as suas operações.

12.1.12. Apresentar um procedimento formal de solicitação de acesso físico e controle da retirada ou instalação de equipamentos.

A CONTRATADA deverá apresentar formalmente sua aderência e cumprimento das normas internacionais de acesso e controle, bem como também na questão ambiental, apresentar o AVCB do local em dia e com as devidas certificações dos órgãos reguladores para as operações das instalações.

13. Testes de segurança

13.1. A CONTRATADA deve permitir que a CONTRATANTE realize os testes de segurança necessários quando solicitado em sistemas, sites, aplicativos, etc. para cumprimento dos objetos deste Contrato.

14. Encerramento do Contrato

14.1. A substituição ou mesmo o término dos serviços prestados pode ocorrer a qualquer momento, para isso alguns itens de segurança da informação devem ser seguidos:

14.1.1. Garantia da revogação dos acessos.

14.1.2. Destruição dos dados armazenados (a menos que a legislação vigente exija a sua conservação, porém os dados deverão ser eliminados assim que o prazo de obrigatoriedade da conservação expirar).

14.1.3. Entrega de todas as gravações telefônicas, capturas de tela, *logs* e quaisquer outros registros armazenados pela CONTRATADA.

15. Penalidades

15.1. Independentemente de eventuais reparações de danos (perdas e danos), a CONTRATANTE poderá efetuar a aplicação de multa não compensatória no valor mínimo de 10% (dez por cento) sobre o valor total do contrato, pelo descumprimento de qualquer regra de segurança prevista neste anexo. Na hipótese de reincidência no descumprimento dos requisitos de segurança, o valor da penalidade poderá ser aplicado em dobro, podendo ser aplicada também a penalidade prevista no Contrato.

16. Vigência e derrogações

16.1. A CONTRATANTE se reserva o direito de alterar os termos e condições durante a vigência do Contrato devido a mudanças nas análises de riscos de segurança. A CONTRATANTE se comunicará com a CONTRATADA via o processo de gestão de terceiros descrito na cláusula 5.

16.2. A CONTRATANTE poderá resolver o Contrato devido a descumprimentos em matéria de segurança dos requisitos definidos neste anexo.

17. Ciência e aceite

Declaro que li e estou disposto a cumprir os requisitos de Segurança Digital dispostos neste documento, aplicáveis ao escopo e às tecnologias relacionadas a este Contrato.

ANEXO II
TERMO DE TRATAMENTO DE DADOS PESSOAIS

1. OBJETIVO

Este Termo de Tratamento de Dados Pessoais ("Termo") aplica-se aos tratamentos de dados pessoais realizados em razão do Contrato de Fornecimento de Bens e Prestação de Serviços ("Contrato"), celebrado entre CONTRATANTE e CONTRATADA, ambas definidas no Contrato, e o integra para todos os fins de direito.

2. DEFINIÇÕES

A CONTRATANTE e a CONTRATADA são doravante designadas, em conjunto, como "Partes" e, individualmente, "Parte".

Não obstante qualquer disposição em contrário no Contrato, no caso de qualquer ambiguidade ou conflito entre os demais documentos integrantes do Contrato e deste Termo, os termos e condições deste Termo prevalecerão.

Quaisquer termos iniciados em letras maiúsculas e não definidos de outra forma neste Termo terão o significado atribuído a eles no Contrato. Exceto conforme modificado abaixo, os termos do Contrato permanecerão em pleno vigor e efeito.

"Anonimização": utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

"Controlador": pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, aqui representado pela CONTRATANTE.

"Dado Pessoal": dado relacionado à pessoa física identificada ou identificável, incluindo números identificativos, dados de localização ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa, bem como nome, sobrenome, estado civil, filiação e endereço, e-mail, telefone.

"Dado Pessoal Sensível": dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófica ou política, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa física.

"Encarregado": pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

"Incidente de Segurança": estabelecido na Cláusula 3.3.1.

"**Leis Aplicáveis**": toda a legislação brasileira, incluindo leis, regulamentos, regras, ordens, decretos ou outras diretrizes com força de lei, relacionada à proteção de dados e que seja aplicável às Partes.

"Operador": pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aqui representado pela CONTRATADA.

"Requisitos de Segurança": requisitos mínimos de segurança da informação estabelecidos pela CONTRATANTE para o Tratamento seguro dos Dados Pessoais. Estarão consolidados em um documento anexo ao Contrato, caso a CONTRATANTE julgue aplicável.

"**Serviços**": os serviços e/ou fornecimentos, bem como outras atividades a serem executadas pela CONTRATADA para a CONTRATANTE, ou em seu nome, nos termos do Contrato.

"Subcontratado": os subcontratados, representantes e outros prestadores de serviços terceirizados, pessoas físicas ou jurídicas, contratados pelo Operador, que tenham acesso a Dados Pessoais relacionados à execução do Contrato.

"Titular dos Dados": pessoa física a quem se referem os dados pessoais que são objeto de tratamento.

"Tratamento": toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

3. OBRIGAÇÕES SOBRE A PROTEÇÃO DE DADOS

3.1. CONTROLADORA E OPERADORA

3.1.1. As Partes reconhecem que, no âmbito da prestação dos Serviços, a CONTRATANTE atuará na qualidade de Controladora, somente, e a CONTRATADA, conforme definido no preâmbulo, na qualidade de Operadora, conforme as obrigações e responsabilidades estabelecidas a cada uma delas, nos termos das Leis Aplicáveis.

3.2. TRATAMENTO DOS DADOS PESSOAIS

3.2.1. São obrigações da CONTRATADA no âmbito deste Termo:

3.2.1.1. Tratar os Dados Pessoais conforme as instruções e diretrizes da CONTRATANTE, na medida do necessário para a prestação do Serviço. É vedado o Tratamento adicional de qualquer Dado Pessoal ao qual a CONTRATADA, porventura, tenha acesso em razão do Contrato para outras finalidades, salvo se expressamente autorizado pela CONTRATANTE.

3.2.1.2. Manter e colocar à disposição, quando solicitado pela CONTRATANTE, o registro de todas as categorias de atividades de Tratamento realizadas em decorrência do Contrato, de acordo com as Leis Aplicáveis. Este registro deverá incluir, ao menos:

a) A descrição dos processos de Tratamento de Dados Pessoais realizados.

b) A relação de transferências de Dados Pessoais para fora do Brasil, quando expressamente autorizadas pela CONTRATANTE, incluindo a identificação (i) dos países de destino e (ii) do mecanismo de transferência utilizado para a realização da transferência internacional.

c) Descrição geral das medidas técnicas e organizacionais utilizadas pela CONTRATADA, conforme descrito nos Requisitos de Segurança, se aplicável.

d) Nome e dados de contato do Subcontratado, se aplicável, assim como seus representantes ou Encarregado.

3.2.1.3. Auxiliar a CONTRATANTE a cumprir as obrigações estabelecidas nas Leis Aplicáveis, principalmente aquelas relacionadas aos direitos dos Titulares dos Dados.

3.2.1.4. Comunicar imediatamente à CONTRATANTE caso os Titulares dos Dados exerçam seus direitos perante a CONTRATADA, sendo vedada qualquer providência para atendimento da demanda dos Titulares dos Dados por Parte da CONTRATADA sem autorização prévia e expressa da CONTRATANTE.

3.2.1.5. Fornecer à CONTRATANTE as informações necessárias para elaboração de documentos exigidos pelas Leis Aplicáveis em decorrência de Tratamentos de Dados Pessoais, especialmente o relatório de impacto à proteção de Dados Pessoais.

3.2.1.6. Permitir que a CONTRATANTE realize auditorias ou inspeções, por si ou por terceiros, a qualquer tempo, mediante comunicação prévia, a fim de verificar o cumprimento das obrigações dispostas neste Termo.

3.2.1.7. Eliminar ou devolver à CONTRATANTE, a critério desta, todos os Dados Pessoais ao término do Contrato.

3.2.1.8. Designar um Encarregado de Proteção de Dados e informar os seus dados de contato à CONTRATANTE, conforme exigível pelas Leis Aplicáveis.

3.3. INCIDENTE DE SEGURANÇA

3.3.1. A CONTRATADA deverá notificar imediatamente a CONTRATANTE: (i) se tiver conhecimento ou suspeitar de qualquer comprometimento, divulgação a pessoas não autorizadas ou uso de Dados Pessoais de maneira não autorizada; (ii) se tiverem sido apresentadas quaisquer reclamações sobre as práticas de tratamento pela CONTRATADA; ou (iii) se tiver ocorrido qualquer descumprimento significativo ou substancial deste Termo (cada um denominado individualmente "Incidente de Segurança").

3.3.2. A CONTRATADA deverá: (i) cooperar integralmente com a CONTRATANTE para a investigação do Incidente de Segurança incluindo, sem limitação, o acesso a servidores para a CONTRATANTE ou o representante por ela designado, para investigação forense com o intuito de determinar o escopo de qualquer Incidente de Segurança; e (ii) preservar todas as informações e evidências relacionadas ao Incidente de Segurança incluindo, entre outros, a suspensão de limpeza (*overwriting*) ou exclusão rotineira de dados ou arquivos de *log*.

3.3.3. A CONTRATADA deverá reembolsar imediatamente à CONTRATANTE todos os custos razoáveis incorridos pela CONTRATANTE para a resposta e/ou minimização do Incidente de Segurança resultantes de ou relacionados à violação pela CONTRATADA de suas obrigações decorrentes do Contrato ou deste Termo.

3.3.4. Salvo quando exigido pelas Leis Aplicáveis ou por uma intimação, ordem judicial ou outro documento legal similar emitido judicialmente ou pela Autoridade Nacional de Proteção de Dados, a CONTRATADA concorda em não divulgar o Incidente de Segurança a qualquer terceiro sem primeiramente obter o consentimento prévio e por escrito da CONTRATANTE.

3.3.5. A critério exclusivo da CONTRATANTE, caso um Incidente de Segurança decorrente de uma violação do Contrato ou deste Termo pela CONTRATADA acarrete a necessidade de (i) envio de uma notificação a autoridades públicas ou indivíduos ou (ii) a adoção de outras medidas corretivas, se solicitado pela CONTRATANTE, a CONTRATADA deverá adotá-las à sua custa. O momento, o conteúdo e a forma de realização de quaisquer notificações ou medidas corretivas serão determinados pela CONTRATANTE.

4. SUBCONTRATAÇÃO

4.1. É vedado à CONTRATADA compartilhar ou permitir o Tratamento por terceiros de Dados Pessoais a que tiver acesso, em decorrência do Contrato, salvo se prévia, expressa e formalmente autorizado pela CONTRATANTE.

4.2. Caso haja subcontratação autorizada pela CONTRATANTE, a CONTRATADA permanecerá responsável por todas as obrigações contidas neste Termo, incluindo:

4.2.1. Informar à CONTRATANTE a identidade e localização do Subcontratado, bem como a descrição do Tratamento pretendido.

4.2.2. Tomar as medidas cabíveis para garantir o cumprimento deste Termo pelo Subcontratado, aplicando a ele as mesmas obrigações e responsabilidades aqui dispostas.

4.3. A CONTRATADA é solidariamente responsável pelo Tratamento de Dados Pessoais realizados pelo Subcontratado, respondendo por eventuais danos causados por este.