1. Requisitos de segurança para SaaS que SEMPRE devem ser utilizados, independentemente da classificação da informação

#	RISCO	CAUSA	REQUISITOS DE SEGURANÇA	Como verificar?
1.1	Violação de conformidade legal	Local de armazenamento das informações	**Localização Geográfica:** os dados, metadados, informações e conhecimento, produzidos ou custodiados, incluindo replicação e cópias de segurança (backups), devem residir em território brasileiro. OBS: quando (1) não houver restrição de acesso legal ao dado **e** (2) não houver disponibilidade do serviço em nuvem no Brasil, é permitido o uso de nuvem no exterior, com: criptografia e gerenciamento de chaves criptográficas que atendam aos requisitos 2.3, para informações CONFIDENCIAIS, e 3.12, para informações INTERNAS. Também é necessário garantir a cópia atualizada dos dados em território brasileiro.	Evidenciar a Região utilizada no provedor de nuvem.
1.2	Perda de informações	Falta ou falha na realização de backup	**Backup:** deve-se realizar backups regulares dos dados. A periodicidade (frequência) do backup deve ser diária | semanal | mensal, o tempo de retenção deve ser de YYY dias. Dados produtivos devem possuir réplica em outra Zona de Disponibilidade. Os dados de backup devem ser protegidos contra adulteração ou acesso indevido, por meio da adoção das melhores práticas e ferramentas de segurança, em especial contra ataques cibernéticos (exemplo: ransomware). OBS: os parâmetros de periodicidade e frequência devem atender ao Recovery Point Objective - RPO, da aplicação. Estes parâmetros devem ser definidos pelo cliente, com o auxílio do PN, devendo ser documentado no procedimento REALIZAR E RECUPERAR BACKUP (Disponível em https://getiki.transpetro.com.br/books/procedimentos-de-infraestrutura/page/realizar-e-recuperar-backup).	Evidenciar os parâmetros utilizados na política de backup aplicada.
1.3	Indisponibilidade da solução	Falha de energia, equipamento, utilidades do datacenter, riscos ambientais.	**Disponibilidade:** a solução contratada deverá possuir disponibilidade mínima (*Service Level Agreement* - SLA) de 99%. OBS 1: 99% de SLA é um valor mínimo sugerido pela SI, caso a necessidade de disponibilidade da solução contratada seja maior que este valor, deve-se colocar o valor adequado. OBS 2: caso haja evidência de que o mercado não consiga entregar o SLA mínimo sugerido de 99%, o cliente da solução deve avaliar e decidir se o valor entregue é suficiente.	Utilizar sistema de monitoração disponibilizado pela TIC.
1.4	Vazamento, alteração ou indisponibilidade da informação	Falhas nos controles de segurança que são de responsabilidadaes do provedor de serviço da Nuvem (Exemplo: AWS, Azure ou GCP)	**Certificações de Segurança:** o provedor de nuvem onde a solução estará hospedada deve possuir as seguintes certificações de segurança para os serviços e regiões envolvidos na solução ofertada. - ISO/IEC 27001; - ISO/IEC 27017; - ISO/IEC 27018; - CSA STAR Level 2.	Apresentar as certificações do provedor de nuvem (AWS, Azure, GCP etc)para as Regiões e Serviços utilizados.
1.5	Vazamento, alteração ou indisponibilidade da informação	Falhas nos controles de segurança que são de responsabilidadaes do provedor de serviço da Nuvem (Exemplo: AWS, Azure ou GCP)	**Relatórios SOC:** a CONTRATADA deverá possuir e, sempre que solicitado pela TRANSPETRO, disponibilizar relatório SOC 2 Tipo 2 do provedor de nuvem para os serviços e regiões onde a solução estará hospedada. OBS 1: se a solução contratada suportar algum processo que esteja no escopo da certificação SOX, tambem deve-se exigir, tanto do provedor de nuvem (AWS, Azure, etc), quanto do provedor da solução de SaaS (Salesforce, Servicenow, etc), a disponibilização de relatório SOC 1 Tipo 2.	Apresentar o relatórios SOC do provedor de nuvem para as Regiões e Serviços utilizados.
1.6	Acesso indevido às informações	Acesso ao disco de armazenamento das informações, seja através do reaproveitamento ou descarte inseguro	**Criptografia em repouso:** os dados em repouso devem ser cifrados utilizando algoritmos de criptografia e tamanhos de chave considerados como seguros pelo padrão NIST SP 800-131A Revision 2 (status approval = "acceptable"). OBS: informações PÚBLICAS não precisam de criptografia.	Apresentar documentação especificando qual o algoritmo e tamanho de chave é utilizado.
1.7	Acesso indevido às informações	Interceptação dos dados durante a transferência para a nuvem	**Criptografia no transporte:** todas as sessões de usuários e outras conexões devem suportar o TLS v1.2 ou superior com *perfect forward secrecy* e sem fixação de certificado (*certificate pinning*), para que a inspeção de tráfego possa operar normalmente.	Listar os protocolos utilizados para as comunicações, como, por exemplo: HTTPS.
1.8	Indisponibilidade do serviço	Encerramento do contrato e impossibilidade de exportação dos dados lock-in ou lock-out	**Portabilidade:** todos os dados estruturados e não estruturados devem estar disponíveis para o cliente e fornecidos a eles mediante solicitação em um formato padrão da indústria (por exemplo, .docx, .xlsx, .pdf, logs e arquivos simples). O fornecedor deve utilizar protocolos de rede padronizados e seguros para a importação e exportação dos dados.	Documentação listando os padrões suportados.
1.9	Acesso indevido às informações	Usuário possuir diversas senhas para memorizar e administrar	**Autenticação**: deve-se utilizar a Federação com o serviço de diretório corporativo no Azure AD, através de SAML 2.0 ou OAuth 2.0/OpenID, de forma que a autenticação seja realizada com o login e senha da própria TRANSPETRO, que terá o controle da política de senhas e exigência de autenticação multifator (*Multi-Factor Authentication* - MFA) para as contas de usuários normais e privilegiados.	Apresentar documentação.
1.10	Acesso indevido às informações	Usuário possuir diversas senhas para memorizar e administrar	**Autenticação**: os acessos de todas as contas de administrador local devem ocorrer através de autenticação multifator (MFA).	Apresentar documentação.
1.11	Abuso ou adulteração das informações	Falha de controle de acesso	**Autorização:** deve ser possível classificar os usuários de acordo com variados perfis e permissões de acesso, conforme os diferentes níveis de permissão que lhes são concedidos. Deve ser possível atribuir as permissões e perfis através de grupos.	Apresentar documentação.
1.12	Acesso indevido às informações ou indisponibilidade do serviço	Exploração de vulnerabilidades WEB	**Web Application Firewall (WAF):** deve-se utilizar proteção de *Web Application Firewall* (WAF) para proteção contra falhas e vulnerabildiades na aplicação Web, incluindo regras de bloqueio contra ataques do OWASP Top 10, como SLQ Injection, CSRF, XSS, etc.	Apresentar documentação.
1.13	Indisponibilidade do serviço	Ataques de negação de serviço (DoS e DDoS)	**AntiDDoS:** deve-se utilizar proteção contra ataques de Negação de Serviço (*Denial of Service* - DoS) e Negação de Serviço Distribuída (*Distributed Denial of Service* - DDoS) através de solução de AntiDDoS nas camadas 3, 4 e 7.	Apresentar documentação.
1.14	Repúdio de ações	Falta de registro de ações	**Registro de logs e tempo de retenção:** a solução deve possuir relatórios e registros de auditoria detalhados que identifiquem o histórico completo de acessos (logins) e ações, por cada usuário ou grupo de usuários, incluindo as contas administrativas e com privilégios. Estes registros devem ser protegidos contra adulteração. Os logs devem ser retidos por 5 anos. OBS: caso haja necessidade de retenção dos logs por mais de 5 anos, seja por exigência do gestor do processo ou por força de normativo vigente, para atendimento a futuras investigações, bem como atendimento de requisições normativas sejam leis ou normas internas, esse tempo deve ser especificado no requisito acima.	Apresentar documentação e parametros de retenção de logs.

1.15	Acesso indevido às informações	Exploração de falhas em API´s	**Proteção de APIs:** quando a solução oferecer Interfaces de Programação de Aplicativos (*Application Program Interfaces* - APIs), elas devem ser projetadas, desenvolvidas, implantadas e testadas de acordo com os principais padrões da indústria (por exemplo, OWASP para aplicativos da Web).	Apresentar documentação.
1.16	Descontinuidade de Negócios	Arquitetura de Recuperação de Desastres Insuficiente	**Continuidade de Negócio:** para aplicações com criticidade Crítica ou Alta, de acordo com o procedimento "Prover Recursos de Infraestrutura de TI" (Disponível em: https://getiki.transpetro.com.br/books/procedimentos-de-infraestrutura/page/prover-recursos-de-infraestrutura-de-ti), é obrigatório que os dados sejam custodiados em pelo menos dois sites distintos com réplicas íntegras dos dados, garantindo alta disponibilidade, baixa latência, escalabilidade, distanciamento geográfico (no mínimo 2 cidades diferentes).	Evidenciar as regiões e zonas de disponibilidades utilizadas pela solução.
1.17	Acesso indevido	Acesso aos dados por autoridades	**Acesso por autoridades:** a CONTRATADA envidará seus melhores esforços para questionar, administrativa ou judicialmente, às suas próprias expensas, solicitações de acesso por autoridades governamentais que não possuam inequívoco respaldo legal, antes de conceder o acesso requerido. Caso a CONTRATADA receba uma solicitação de acesso emitida por uma autoridade governamental, do Brasil ou do exterior, aos dados da TRANSPETRO armazenados em decorrência do Contrato, deverá dar ciência imediata à TRANSPETRO, ressalvadas as hipóteses legais de sigilo na investigação e desde que expressamente exigido, por escrito, pela autoridade.	N/A.
1.18	Uso indevido	Uso indevido das informações pelo provedor	É proibido o uso de informações da TRANSPETRO pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado.	N/A.
1.19	Vazamento, alteração ou indisponibilidade da informação	Configuração incorreta na plataforma de nuvem	**CSPM:** deve-se utilizar uma solução de Gerenciamento de Postura de Segurança de Nuvem (Cloud Security Posture Management - CSPM) e os alertas de segurança reportados por esta solução devem ser tratados.	Informar a solução de CSPM utilizada e evidenciar que os alertas foram tratados.
1.20	Vazamento, alteração ou indisponibilidade da informação	Vulnerabilidade nas cargas de trabalho de nuvem	**CWP:** deve-se utilizar uma solução de Proteção das Cargas de Trabalho de Nuvem (Cloud Workload Protection - CWP) e os alertas de segurança reportados por esta solução devem ser tratados.	Informar a solução de CWP utilizada e evidenciar que os alertas foram tratados.

2. Quando o SaaS processar informações CONFIDENCIAIS e/ou PESSOAIS SENSÍVEIS*, utilizar estes requisitos adicionais:

***Pessoal sensível de acordo com LGPD ou informação pessoal relativa a honra, imagem, intimidade e vida privada.**

#	RISCO	CAUSA	REQUISITOS DE SEGURANÇA	Como verificar?
2.1	Vazamento, alteração ou indisponibilidade da informação	Falhas nos controles de segurança que são de responsabilidadaes do fornecedor de SaaS (Exemplo: Salesforce, Servicenow etc)	**Certificação de Segurança:** o fornecedor da solução de SaaS deve possuir a certificação de segurança ISO/IEC 27001 para o serviço prestado para a TRANSPETRO. OBS: este requisito não é igual ao 1.4. Lá a certificação ISO 27001 exigida é do provedor de nuvem pública onde a solução será hospedada (AWS, Microsoft Azure, Google Cloud etc), aqui a certificação exigida é do fornecedor de SaaS (Salesforce, Servicenow, Office 365 etc).	Apresentar a certificação para a solução ofertada (Salesforce, Servicenow etc).
2.2	Vazamento, alteração ou indisponibilidade da informação	Falhas nos controles de segurança que são de responsabilidadaes do fornecedor de SaaS (Exemplo: Salesforce, Servicenow etc)	**Certificação de Segurança:** o fornecedor da solução de SaaS deve possuir a certificação de segurança ISO/IEC 27018 para o serviço prestado para a TRANSPETRO. Além disso, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto. OBS 1: este requisito só é válido se houver tratamento de informações PESSOAIS SENSÍVEIS ou informação pessoal relativa à intimidade, vida privada, honra e imagem. OBS 2: este requisito não é igual ao 1.4. Lá a certificação ISO 27018 exigida é do provedor de nuvem pública onde a solução será hospedada (AWS, Microsoft Azure, Google Cloud etc), aqui a certificação exigida é do fornecedor de SaaS (Salesforce, Servicenow, Office 365 etc).	Apresentar a certificação para a solução ofertada (Salesforce, Servicenow etc).
2.3	Acesso indevido às informações	Acesso indevido as informações por falha no processo de gerenciamento de chaves criptográficas	**Gerenciamento de chaves criptográficas:** deve ser permitido a utilização de chave gerada e gerenciada pelo próprio cliente (*Bring Your Own Key - BYOK*). Estas chaves deverão ser armazenadas em solução de *Hardware Security Module* (HSM), que atenda o padrão FIPS 140-2 **Level X**. OBS 1: quando o armazenamento da informação for no exterior, o HSM que armazena as senhas deve atender ao Level 3 do FIPS 140-2. Quando for no Brasil, deve-se atender ao Level 2 do FIPS 140-2. OBS 2: caso a solução não possua suporte a BYOK, esta função pode ser substituída por um controle compensatório, como a existência das certificações de segurança ISO 27001, 27017, 27108, CSA STAR Level 2 ou relatório SOC 2 Tipo 2. Outros controles compensatórios podem ser aceitos mediante avaliação do time de SI, através de pedido de parecer de segurança.	Apresentar documentação.

3. Quando o SaaS NÃO processar informações CONFIDENCIAIS e/ou PESSOAIS SENSÍVEIS*, utilizar estes requisitos adicionais:

#	RISCO	CAUSA	REQUISITOS DE SEGURANÇA	Como verificar?
3.1	Vazamento, alteração ou indisponibilidade da informação	Ausência de política de segurança	**Política de Segurança:** o fornecedor da solução de SaaS deve possuir um conjunto de políticas de segurança da informação definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia. Uma política disciplinar ou de sanção formal deve ser estabelecida para funcionários que violaram políticas e procedimentos de segurança.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.
3.2	Vazamento, alteração ou indisponibilidade da informação	Falhas nos controles de segurança que são de responsabilidadaes do fornecedor de SaaS(Exemplo: Salesforce, Servicenow etc)	**Proteção do ambiente de nuvem:** o fornecedor da solução de SaaS deve gerenciar a postura de segurança do ambiente de nuvem onde o serviço é hospedado e também deve proteger as cargas de trabalho, aplicando políticas que reflitam as boas práticas de segurança e tratando os alertas relacionados a não conformidades e vulnerabilidades indicadas por estas plataformas.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.
3.3	Vazamento, alteração ou indisponibilidade da informação	Falha nos procedimentos de gerenciamento de identidade e controle de acesso	**Gerenciamento de Identidade e Acesso:** controles de gerenciamento de identidade e acesso devem estar implementados e gerenciados, incluindo o acesso às ferramentas de auditoria, ciclo de vida e provisão de credenciais, segregação, acesso ao código fonte, acesso de terceiros, fontes confiáveis, autorização, revisão e revogação de acessos de usuários e credenciais.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.
3.4	Vazamento, alteração ou indisponibilidade da informação	Falhas introduzidas por mudanças no ambiente	**Gestão de Mudanças e de Configurações:** controles de alterações e gerenciamento de configurações devem ser implementados e gerenciados, incluindo novos desenvolvimentos, aquisição, desenvolvimento terceirizado, testes de qualidade, instalação de softwares e mudanças na produção.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.
3.5	Acesso indevido às informações ou indisponibilidade do serviço	Falhas de configuração do sistema operacional de responsabilidade do fornecedor de SaaS (Exemplo: Salesforce, Servicenow etc).	**Fortalecimento (*hardening*) de Sistema Operacional:** se a solução for composta por instâncias ou máquinas virtuais, o fornecedor da solução de SaaS deve garantir que todo sistema operacional deve ser reforçado para fornecer apenas portas, protocolos e serviços necessários para atender às necessidades de negócios e ter suporte aos controles técnicos, tais como: antivírus, monitoramento de integridade de arquivos e criação de log como parte de seu padrão ou modelo básico de construção operacional.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.

3.6	Acesso indevido às informações ou indisponibilidade do serviço	Exploração de vulnerabilidades técnicas	**Gestão de Vulnerabilidades e Aplicação de Patches:** processos de gestão de vulnerabilidades e de aplicação de patches devem estar estabelecidos para identificar e corrigir vulnerabilidades no ambiente.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.
3.7	Acesso ou alteração indevida às informações	Falhas na aplicação/software	**Desenvolvimento Seguro:** o desenvolvedor da solução deverá possuir políticas e procedimentos estabelecidos para o desenvolvimento seguro, controle de mudança dos sistemas, segregação do ambiente de desenvolvimento e produção, testes de segurança, aceitação, e proteção dos dados em ambiente de produção.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.
3.8	Acesso indevido às informações ou indisponibilidade do serviço	Alterações indevidas em ambiente de produção	**Segregação entre ambientes produtivos e não-produtivos:** os ambientes de produção e não produção devem ser separados para impedir o acesso não autorizado ou alterações nos ativos de informação. A separação dos ambientes pode incluir: firewalls de inspeção com informações de estado, fontes de autenticação de domínio / domínio e separação clara de tarefas (segregação de função) para pessoas que acessam esses ambientes como parte de suas obrigações de trabalho.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.
3.9	Acesso indevido às informações	Acesso pelo provedor ou outros clientes	**Isolamento entre clientes ou *tenants*:** O acesso intra-tenant deve ser adequadamente segmentado e segregado, monitorado e restrito de outros tenants. Políticas, procedimentos e melhores práticas devem estar estabelecidas para garantir o isolamento entre clientes e o acesso indevido aos dados pelo próprio provedor.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.
3.10	Acesso indevido às informações	Descarte inseguro e ambientes não produtivos	**Descarte seguro:** os dados de produção não devem ser replicados ou usados em ambientes de não produção. Políticas e procedimentos devem ser estabelecidos para o descarte seguro e a remoção completa de dados de todos os meios de armazenamento, garantindo que os dados não sejam recuperáveis por qualquer meio forense computacional.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.
3.11	Acesso indevido às informações	Risco de pessoal	**Recursos Humanos:** controles de gerenciamento de recursos humanos devem estar implementados e gerenciados incluindo retorno de ativos, seleção, contratos, rescisão, acordos de não divulgação, gerenciamento de dispositivos móveis, papéis e responsabilidades, uso aceitável de tecnologia, treinamento e conscientização e responsabilidades dos usuários.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.
3.12	Acesso indevido às informações	Acesso às informações pelo provedor de acesso	**Gerenciamento de chaves de criptografia:** para informação com classificação INTERNA, é permitida a utilização de chave gerada e gerenciada pelo próprio provedor. OBS: quando o armazenamento for no exterior, as chaves de criptografia devem ser armazenadas em um HSM.	Apresentar política, procedimento ou declaração de que atente a estes requisitos.

4. Requisitos para conexão de rede entre o SaaS e a Rede Integrada Corporativa (RIC) da Petrobras

#	RISCO	CAUSA	REQUISITOS DE CONEXÃO DE REDE	Como verificar?
4.1	Ataque cibernético para redes da PETROBRAS na RIC ou nuvem.	Ataques vindos de outras redes	**Firewall:** para interconexão do ambiente de SaaS com a rede PETROBRAS, deve-se utilizar firewall do lado da rede PETROBRAS, seja na RIC ou na nuvem Azure, com regras restritivas, bloqueando todo o tráfego e liberando somente o que for necessário (regras *default-deny*). Obs: este requisito é válido se houver necessidade de integração entre o ambiente de SaaS com a RIC ou com as nuvens da TRANSPETRO na Azure.	N/A
4.2	Ataque cibernético para redes da PETROBRAS na RIC ou nuvem.	Ataques vindos de outras redes	**IPS:** para interconexão do ambiente de SaaS com a rede PETROBRAS, deve-se utilizar um *Intrusion Prevention System* - IPS para inspecionar todo o tráfego. Este IPS deverá abrir os pacotes criptografados para realizar a inspeção. Obs: este requisito é válido se houver necessidade de integração entre o ambiente de SaaS com a RIC ou com as nuvens da TRANSPETRO na Azure.	N/A
4.3	Acesso indevido aos dados	Interceptação da comunicação	**Criptografia:** toda a comunicação entre estas redes deve ser criptografada. Obs: este requisito é válido se houver necessidade de integração entre o ambiente de SaaS com a RIC ou com as nuvens da TRANSPETRO na Azure.	N/A

5. Evidências do atendimento dos requisitos de segurança

#	RISCO	CAUSA	REQUISITOS DE CONEXÃO DE REDE	Como verificar?
5.1	N/A	N/A	A TRANSPETRO poderá, a qualquer momento ao longo da vigência do contrato, solicitar evidências de atendimento de qualquer um dos requisitos de segurança especificados.	N/A