PLANO DE SEGURO DE SEGURANÇA

STATUS: VALIDADO

Versão: 2.0

PÚBLICO	INTERNO	RESTRITO	SIGILOSO
X			

SUMÁRIO

GENERALIDADES

APRESENTAÇÃO DO PLANO DE SEGUROS DE SEGURANÇA

Este Plano de Seguro de Segurança (“SIP”) se aplica a qualquer terceiro (“Terceiro”) que acesse o Sistema de Informações ou Dados do Bureau Veritas (por exemplo, ao fornecer um serviço ao Bureau Veritas ou ao desenvolver uma parceria digital).

O objetivo é garantir que terceiros atendam às necessidades de segurança do Bureau Veritas e estejam alinhados às melhores práticas de segurança no acesso ao Sistema de Informação ou Dados do Bureau Veritas.

Isso garante que o Bureau Veritas Data seja devidamente protegido e seus sistemas permaneçam eficazes, robustos e resilientes.

Este SIP deve incluir medidas de segurança e controles necessários a serem aplicados e mantidos no escopo do serviço oferecido ou parceria desenvolvida com o Bureau Veritas.

Solicita-se ao Terceiro que preencha devidamente o presente documento e forneça comentários e detalhes apropriados para ajudar o Bureau Veritas a avaliar sua postura de segurança. Em caso de não cumprimento de um requisito, é do interesse do Terceiro estabelecer medidas alternativas, se houver, que eles implantem para reduzir o risco.

Ao receber este documento preenchido, o Bureau Veritas irá analisá-lo e se reserva o direito de solicitar outras provas quanto à aplicabilidade/conformidade com os requisitos de segurança expressos.

Um SIP preenchido com entradas de terceiros do Bureau Veritas torna-se um documento restrito (C3). Depois de preenchido, o nível de classificação no rodapé do documento deve ser atualizado em conformidade.

ESCOPO E DURAÇÃO

Em relação ao Código de Conduta do Bureau Veritas Partners, o SIP é parte integrante da relação contratual entre o **Bureau Veritas** e:

Nome da empresa	
Endereço da Empresa	
Detalhes do ponto de contato	

O SIP descreve as medidas de segurança técnicas e organizacionais, implementadas pelo Terceiro, para proteger a si próprios e ao Bureau Veritas Data contra processamento ilegal, perda, roubo, exclusão acidental ou fraudulenta, alteração ou destruição, ou dano, ou uso ou divulgação não autorizada.

Estas medidas de segurança são aplicáveis ao seguinte escopo de serviço prestado a/ parceria desenvolvida com o Bureau Veritas:

Eles permanecerão em vigor por toda a duração do contrato subjacente firmado com o Bureau Veritas.

Como parte das políticas do Bureau Veritas, o Bureau Veritas reserva-se o direito de auditar a conformidade dos Terceiros com as disposições de segurança indicadas no SIP.

REVISÃO DE TERCEIROS

O Bureau Veritas realiza avaliações regulares de seus terceiros. Posteriormente, uma revisão regular do SIP será realizada no máximo uma vez por ano.

Solicitamos ao Terceiro que atualize o presente documento, forneça um documento de suporte atualizado e informe o Bureau Veritas sobre qualquer alteração que afete sua postura de segurança ou sua capacidade de proteger os dados do Bureau Veritas.

Data da última revisão:	

REQUISITOS DE SEGURANÇA

ORGANIZAÇÃO E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO	
O Terceiro deve ter um funcionário identificado, responsável pelo gerenciamento geral da segurança da informação.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	
O Terceiro deverá formalizar uma Política de Segurança da Informação. A política deve abordar princípios de governança precisos e requisitos de segurança fundamentais a serem adotados para fornecer um serviço seguro. A política deve ser comunicada às partes relevantes e atualizada regularmente.	☐ Compatível ☐ Parcialmente compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

CERTIFICAÇÃO DE TERCEIROS	
O Terceiro deverá: ▪ Informar o Bureau Veritas de quaisquer certificados ou provas de conformidade com um ou vários padrões de segurança da informação (por exemplo, ISO, NIST, etc.); ▪ Descreva o escopo dos certificados; ▪ Compartilhe com o Bureau Veritas os certificados ou qualquer outra prova de conformidade.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de Terceiros:	

SUBCONTRATAÇÃO	
O Terceiro deverá identificar e compartilhar a lista de subcontratados que apoiam na prestação de serviços ao Bureau Veritas. O terceiro deve, por meio de um processo formal, avaliar e garantir que os subcontratados que lidam com as informações do Bureau Veritas cumpram os mesmos requisitos de segurança que o terceiro.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de Terceiros:	

DISPOSIÇÕES ADICIONAIS DE PRIVACIDADE E SEGURANÇA	
O Terceiro deverá comunicar ao Bureau Veritas os documentos e comprovações necessários (por exemplo, relatório de auditoria de segurança, varreduras de vulnerabilidade, etc.) demonstrando que os requisitos e questões de segurança foram adequadamente tratados. O Terceiro deve fornecer ao Bureau Veritas as informações necessárias e acesso para realizar uma auditoria de segurança, se não for recente o relatório de auditoria é fornecido pelo Terceiro.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

RECURSOS HUMANOS

TREINAMENTO E CONSCIENTIZAÇÃO DE SEGURANÇA	
O Terceiro deverá garantir que seus funcionários que intervêm nas instalações do Bureau Veritas ou manipulam os Dados do Bureau Veritas sejam treinados para cumprir os requisitos de segurança e as melhores práticas. O Terceiro deverá compartilhar evidências de que sua empresa mantém ações e campanhas regulares de conscientização.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

RESPEITO ÀS POLÍTICAS DO BUREAU VERITAS	
Os funcionários terceirizados com acesso aos sistemas e infraestrutura do Bureau Veritas devem reconhecer e aceitar o uso dos recursos do Bureau Veritas com relação às políticas e controles do Bureau Veritas deste documento.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

ACESSO LÓGICO

ACESSO LÓGICO A RECURSOS E DADOS DE TI	
O Terceiro deverá manter medidas de segurança adequadas para proteger contra o acesso ilegal e não autorizado ao Bureau Veritas Data, recursos usados para fornecer o serviço ou colaborar com o Bureau Veritas. Essas medidas devem incluir (mas não se limitam a): ▪ Usando contas nominativas; ▪ Concessão de direitos de acesso com base na necessidade de conhecer o principal; ▪ Métodos de autenticação individual devem ser usados para validar a identidade dos usuários; ▪ Aplicar uma política de senha forte; ▪ Revise os direitos de acesso regularmente.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

GESTÃO DE CONTA PRIVILEGIADA	
O Terceiro deverá gerenciar contas privilegiadas com acesso aos dados do Bureau Veritas e monitorar rigorosamente sua atividade. O método de autenticação adotado para contas privilegiadas deve ser mais forte em comparação com contas regulares (por exemplo, uso de autenticação multifator, política de senha mais forte, etc.).	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

SISTEMA DE AUTENTICAÇÃO	
O acesso aos serviços e sistemas de terceiros para funcionários do Bureau Veritas deve ser feito por meio do diretório corporativo, usando um Single Sign-On (SSO) entre o Bureau Veritas e o terceiro. Se não for possível, o Terceiro deve ajudar o Bureau Veritas a redigir um procedimento de gerenciamento de conta que descreve (mas não se limita a): ▪ Criação de contas; ▪ Política de Senhas; ▪ Comunicação de senha inicial; ▪ Atribuição/modificação/exclusão de autorizações.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

SEGURANÇA DE INFRAESTRUTURA, REDE E SISTEMAS

MEDIDAS DE PROTEÇÃO	
O Terceiro deverá implementar medidas técnicas e organizacionais suficientes para proteger os recursos usados para fornecer o serviço ao Bureau Veritas e os equipamentos que hospedam/manipulam os Dados do Bureau Veritas. As seguintes medidas devem ser consideradas: ▪ Segmentação adequada da rede; ▪ Implementar firewalls para proteger diferentes redes e recursos; ▪ Implementando um produto de Detecção e Prevenção de Intrusão em hospedeiros e monitorando alertas ativamente; ▪ Servidores de proteção que hospedam dados e aplicativos; ▪ Proteja os servidores usando software antivírus atualizado regularmente ou sistema operacional ("SO") apropriado contramedidas contra vírus; ▪ Garantir que os sistemas operacionais sejam mantidos e atualizados, bem como os aplicativos instalados neles; ▪ Varredura regular de rede e hosts para detectar qualquer configuração não autorizada ou vulnerável (varredura de vulnerabilidade); ▪ Implementar e manter tecnologias de filtragem de web e proteção de e-mail.	☐ Compatível ☐ Parcialmente compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

PROTEÇÃO DE PONTO FINAL	
O Terceiro deve implementar medidas técnicas e organizacionais suficientes para proteger as estações de trabalho dos funcionários, laptops e outros dispositivos que eles usam para cumprir suas missões. As seguintes medidas devem ser consideradas: ▪ Usando Sistemas Operacionais atualizados e devidamente configurados (“SO”); ▪ Proteja os dispositivos finais usando produtos antivírus e antimalware e atualize-os regularmente; ▪ Garantir que as soluções antivírus e antimalware sejam nunca desativado em dispositivos finais, a menos que necessário; ▪ Garantir que o acesso aos dispositivos seja protegido (por exemplo, por senha individual); ▪ Implementar e manter a filtragem da web e tecnologias de proteção de e-mail.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

MONITORAMENTO E REGISTRO

MONITORAMENTO E REGISTRO CONTÍNUO	
O Terceiro deverá adotar medidas para monitorar e registrar continuamente quaisquer eventos de segurança (por exemplo, tentativa de acesso não autorizado) no Bureau Veritas Data, bem como a infraestrutura e os sistemas usados no escopo do contrato. O nível dos registros registrados deve garantir a responsabilidade pelas ações realizadas e o acesso aos dados do Bureau Veritas. O Bureau Veritas poderá solicitar registros de acesso aos seus Dados. Esses registros devem ser usados para fins de investigação. O Terceiro deverá compartilhar as modalidades pelas quais o Bureau Veritas pode solicitar Logs.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

MONITORAMENTO E REGISTRO CONTÍNUO	
O Terceiro deve correlacionar e analisar continuamente os registros para detectar incidentes de segurança, vazamentos de dados ou quaisquer eventos que possam comprometer a segurança dos Dados e serviços.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

DESENVOLVIMENTO E MANUTENÇÃO SEGUROS

DESENVOLVIMENTO SEGURO	
O Terceiro deve respeitar as práticas de desenvolvimento seguro ao desenvolver aplicativos em nome do Bureau Veritas. Essas práticas de desenvolvimento seguro devem levar em consideração as recomendações de referências aclamadas (por exemplo, OWASP).	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

DOCUMENTAÇÃO OPERACIONAL	
O Terceiro deverá manter e atualizar regularmente a documentação adequada e suficiente do aplicativo e dos serviços. Os elementos da documentação devem ser acordados com o Bureau Veritas. Os seguintes elementos devem ser considerados: ▪ Diagrama da arquitetura; ▪ Fluxos de rede; ▪ Lista dos ambientes de Produção e Pré-produção, sua finalidade e medidas de segurança aplicadas para protegê-los; ▪ Ciclos funcionais e técnicos de remendo; ▪ Documentação operacional para manuseio do aplicativo. O Bureau Veritas deve exigir cópias da documentação regularmente.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

SEGURANÇA FÍSICA E AMBIENTAL

CONTROLES DE SEGURANÇA FÍSICA E AMBIENTAL	
O Terceiro deverá implementar medidas e controles suficientes para proteger a segurança física das instalações que hospedam o Bureau Veritas Data. Essas medidas e controles devem proteger o Terceiro instalações contra acessos não autorizados, bem como ameaças externas e ambientais. As seguintes medidas devem ser consideradas: ▪ Portões que dão acesso a áreas privadas e áreas de hospedagem de dados bloqueados; ▪ Limite o acesso apenas a funcionários autorizados; ▪ Proteção contra intrusão (alarmes e vídeo vigilância, sistema de detecção de intrusão, guardas); ▪ Medidas impostas para controlar o acesso às salas dos servidores (controles de acesso individuais); ▪ Visitantes identificados e acompanhados durante as visitas; ▪ Procedimentos em vigor para garantir que o ambiente problemas (inundação, incêndio, terremotos, etc.) não causam uma interrupção no serviço ou perda de dados.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

PROTEÇÃO DE DADOS DO BUREAU VERITAS

LOCALIZAÇÃO E ACESSO DE DADOS	
O Terceiro deve definir a localização geográfica de seus datacenters ou de seu Terceiro na nuvem (ou seja: AWS) onde os Dados do Bureau Veritas serão armazenados. O Terceiro deverá ser capaz de identificar individualmente os funcionários e máquinas com acesso ao Bureau Veritas Data.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

BACKUPS DE DADOS	
O Terceiro deverá formalizar um procedimento de backup e testá-lo regularmente. Os dados do Bureau Veritas devem ser copiados. As regras de retenção e backup devem ser definidas com o representante do Bureau Veritas, se necessário, a fim de atender às necessidades do negócio. Os backups devem ser replicados em um site secundário. Todos os dados devem ser armazenados, submetidos a backup e eliminados de acordo com as leis e regulamentos de proteção de dados aplicáveis e as obrigações contratuais.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

CRIPTOGRAFIA DE DADOS	
O Terceiro deve garantir que os Dados do Bureau Veritas estejam protegidos contra acesso não autorizado. A criptografia de dados deve ser realizada quando solicitada pelo Bureau Veritas. O Terceiro compromete-se a criptografar os Dados do Bureau Veritas em trânsito em redes públicas externas, incluindo a Internet. As trocas de dados devem ser realizadas usando protocolos seguros e devidamente configurados (SFTP, TLS). Além disso, a criptografia deve ser implantada em computadores e dispositivos finais que contenham dados confidenciais do Bureau Veritas.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

DESTRUIÇÃO DE DADOS	
O Terceiro deverá formalizar um procedimento de destruição de Dados para destruição final de Dados após a expiração ou rescisão do contrato e consentimento do Bureau Veritas. O procedimento de destruição deve garantir que os dados do Bureau Veritas não possam ser recuperados por terceiros após a exclusão final.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

GERENCIAMENTO DE INCIDENTES DE SEGURANÇA

PROCESSO DE GESTÃO DE INCIDENTES	
O Terceiro deve implementar um processo de resposta a incidentes de segurança, bem como mecanismos para compartilhar informações durante e após um incidente. O terceiro deve descrever: ▪ O escopo do incidente de segurança da informação que eles informarão ao Bureau Veritas; ▪ O nível de informação divulgado ao Bureau Veritas; ▪ Janela de tempo para relatar os incidentes de segurança; ▪ O procedimento de notificação; ▪ Informações de contato específicas; ▪ Soluções existentes que podem ser aplicadas em alguns casos de incidentes de segurança. O processo de gestão de incidentes deve respeitar as leis e regulamentos aplicáveis (por exemplo, notificação às autoridades locais com atrasos).	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

RELATÓRIO DE INCIDENTES	
O Terceiro e o Bureau Veritas devem concordar com os mecanismos e canais de comunicação que permitem: ▪ O Bureau Veritas deve relatar os eventos de segurança da informação detectados ao Terceiro; ▪ O Terceiro deve relatar os eventos de segurança da informação detectados ao Bureau Veritas; ▪ Bureau Veritas para rastrear o status de um evento de segurança da informação relatado.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

NÍVEL DE SERVIÇO E CONTINUIDADE

PLANO DE CONTINUIDADE DOS NEGÓCIOS	
O Terceiro deverá formalizar um plano de continuidade de negócios para garantir a continuidade do serviço prestado ao Bureau Veritas durante uma situação adversa, em conformidade com o nível de serviço definido em contrato (SLAs).	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

CONFORMIDADE

CONFORMIDADE COM A GDPR	
O Terceiro deve cumprir as leis e regulamentos de proteção de dados pessoais aplicáveis, incluindo o GDPR. Em particular, o Terceiro deverá implementar medidas técnicas e organizacionais adequadas para proteger os Dados do Bureau Veritas, incluindo dados pessoais.	☐ Compatível ☐ Parcialmente Compatível ☐ Não Compatível ☐ Não se Aplica
Comentários de terceiros:	

Glossário

CISO significa Diretor de Segurança da Informação.

Dados (ou Dados do Bureau Veritas) significam os dados, arquivos e conteúdo pertencentes ao Bureau Veritas, incluindo Dados Pessoais.

GDPR significa o Regulamento Geral de Proteção de Dados da UE 2016/679 de 27 de abril de 2016. O regulamento visa garantir a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Sistema de Informação significa conjunto integrado de componentes (incluindo equipamento de TI) para coletar, armazenar e processar Dados e fornecer informações.

ISS significa Segurança do Sistema de Informação.

Políticas ISS significam Políticas de Segurança do Sistema de Informação que incluem o ISSP Global e as Políticas Operacionais. Conjunto de documentos que definem o enquadramento da Segurança do Sistema de Informação (ISS) através de princípios de governação e regras pragmáticas, que serão implementados em todo o Grupo Bureau Veritas.

LDAP significa Lightweight Directory Access Protocol (Protocolo de Acesso a Diretórios Leves).

Malware significa (abreviação de software malicioso) qualquer software usado para interromper as operações do computador ou móvel, coletar informações críticas, obter acesso ao sistema de informações privado ou exibir publicidade indesejada. O termo se refere a uma variedade de formas de software hostil ou intrusivo, incluindo vírus de computador, worms, cavalos de Tróia, ransomware, spyware, adware, scareware e outros programas maliciosos.

NDA significa Acordo de Não Divulgação.

Informações Pessoais significa qualquer informação relacionada a uma pessoa física identificada ou identificável ("titular dos dados"); uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como nome, número de identificação, dados de localização, identificador on-line ou a um ou mais fatores específicos de natureza física, fisiológica, identidade genética, mental, econômica, cultural ou social dessa pessoa natural

SFTP significa Secure File Transfer Protocol (Protocolo de Transferência Segura de Arquivos).

SIP significa Security Insurance Plan (Plano de Seguro de Segurança).

TLS significa Transport Layer Security (Segurança da Camada de Transporte). É um protocolo criptográfico que protege as comunicações ponta a ponta nas redes.

Terceiro significa qualquer parte não pertencente ao grupo do Bureau Veritas, incluindo, mas não se limitando a prestadores de serviços, parceiros, subcontratados ou clientes.

Aprovador

Nome	Posição	Data
Julien ANICOTTE	Grupo CISO	13/10/2020
Sonia DELPY	Grupo DPO	13/10/2020

Versões

Versão	Autor	Natureza das modificações	Data
1.0	Meryem OUKEMENI	Validação e Difusão	27/07/2018
2.0	Youness TASTIFT	Revisão do SIP	09/10/2020