1. **Objetivo**

Estabelecer as diretrizes e procedimentos para gestão de acessos (concessão e revogação de acessos), desenvolvimento de sistemas, suporte ao usuário, novas tecnologias, infraestrutura de redes, sistemas e aplicações, servidores e serviços, proposição e suporte de mudanças e operações diversas. Para preservar as informações da São Paulo Turismo S/A quanto à: Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais; confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas; e disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

1. **Abrangência**

As definições, diretrizes e demais orientações introduzidas por esta norma atende aos funcionários da SP Turismo e ao seu público externo.

1. **Definições**
	1. Active Directory: Uma implementação de serviço de diretório no protocolo LDAP que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações a usuários e administradores desta rede.
	2. Comitê de Segurança da Informação: Comissão responsável por gerenciar assuntos relacionados à Segurança da Informação, composto por colaboradores da GTI da SP Turismo.
	3. Datacenter: Centro de processamento de dados.
	4. CDS: Coordenadoria de Desenvolvimento de Sistemas.
	5. CI: Correspondência Interna.
	6. CRS: Coordenadoria de Redes e Segurança da Informação.
	7. ERP Protheus: Sistema de Gestão Empresarial.
	8. GIT: Um sistema de controle de versão de arquivos. Através do qual se desenvolve projetos na qual diversas pessoas podem contribuir simultaneamente, editando e criando novos arquivos e permitindo que estes possam existir sem o risco de suas alterações serem sobrescritas.
	9. GRH: Gerência de Recursos Humanos.
	10. GSS: Gerência de Segurança e Serviços Auxiliares.
	11. GTI: Gerência de Tecnologia da Informação.
	12. LTO 5: Uma fita magnética com o objetivo de armazenamento não-volátil, isto é, uma vez os dados gravados esses são conservados.
	13. Redmine: Um software livre, gerenciador de projetos baseados na web e ferramenta de gerenciamento de bugs. Contém calendário e gráficos de Gantt para ajudar na representação visual dos projetos e seus deadlines (prazos de entrega). Pode também trabalhar com múltiplos projetos.
	14. SAI: Sistema Integrado de Automação.
	15. SAN: Storage Area Network.
	16. SCRUM: Metodologia ágil para gestão e planejamento de projetos de software.
	17. Trello: Ferramenta de gerenciamento de projetos em listas extremamente versátil e que pode ser ajustada de acordo com as necessidades do usuário. Pode utilizá-lo para organizar as tarefas do trabalho, os planos de viagens, as prioridades de estudos, entre muitos outros.
	18. VLAN: Uma rede local virtual, logicamente independente.
2. **Diretrizes**
	1. **Gestão de desenvolvimento/mudanças**
		1. O serviço de desenvolvimento de sistemas on-line e sistemas web deve atender às demandas de toda a SP Turismo através da análise, desenvolvimento e manutenção de páginas web corporativas, projetos turísticos, páginas de programas institucionais, sistemas de controle e pesquisa, dentre outras.
		2. Toda a atividade deve ser realizada internamente pela equipe de desenvolvimento da GTI (Gerência de Tecnologia da Informação), de acordo com as necessidades das unidades de negócio, incluindo as questões relacionadas ao ERP Protheus.
		3. As solicitações de desenvolvimento devem ser feitas pelas áreas e originadas através de uma reunião inicial com a equipe de desenvolvimento e sistemas para avaliar a solicitação em questão.
		4. Como metodologia para o desenvolvimento, a GTI deve se basear nas premissas da metodologia SCRUM para desenho e codificação em todos os ciclos da análise e desenvolvimento das aplicações.
		5. Caso uma solicitação seja viável (considerando orçamento, prazo e resultados) de acordo com a análise do Gerente de TI e do Gestor de Negócio da área solicitante (confirmar), a formalização da solicitação do desenvolvimento deve ser iniciada com a elaboração da Solicitação de Desenvolvimento (vide Anexo I) pela GTI contendo o detalhe a ser realizado.
		6. Este documento deve ser enviado para área solicitante que realiza a revisão das informações destacadas para validação e assinatura.
		7. Com o documento assinado e aprovado, a GTI pode iniciar as atividades de desenvolvimento. Caso exista uma necessidade de correção ou adequação de algum elemento, esta deve ser adicionada como incrementos do documento de Solicitação de Desenvolvimento do projeto.
		8. A GTI deve realizar a alteração em um ambiente de teste, controlando o versionamento de aplicações e códigos desenvolvidos, através da ferramenta GIT e de repositórios criados para esse fim.
		9. Todo ciclo (SPRINT) que é terminado, deve ser entregue para validação da área requisitante do teste da mudança requisitada.
		10. Caso o teste seja efetivo, a área solicitante deve aprovar a mudança. O Gerente de TI ou por pessoa a quem por ele tenha sido delegada essa atribuição também deve aprovar. Em seguida a mudança deve ser implementada pelo o desenvolvedor no ambiente de produção.
		11. A responsabilidade pela aprovação final, antes de qualquer alteração ser aplicada ao ambiente de produção, deve ser da gerência GTI ou por pessoa a quem por ele tenha sido delegada essa atribuição. Também deve aprovar as mudanças.
		12. Adicionalmente deve ser utilizada a ferramenta de controle de projetos Redmine que se integra a ferramenta GIT que visa controlar e registrar junto a ferramenta online Trello, para efeito de histórico do projeto, todas as mudanças implementadas no projeto.
		13. Tal qual o processo de desenvolvimento de uma nova aplicação, as mudanças também devem passar pelo processo de aprovação e, por fim, validação, antes de serem instaladas no ambiente de produção.
		14. Caso um projeto possua requisitos fechados e não exija uma interação mais frequente entre a CDS (Coordenadoria de Desenvolvimento de Sistemas) e a área requisitante, o uso do GIT/Redmine/Trello deve ser restrito ao time de desenvolvimento (empresa terceira ou interna).
		15. Para os casos onde se faz necessária a interação mais frequente, envolvendo inclusive a participação de externos, a ferramenta Trello deve ser utilizada.
		16. Para garantia de funcionamento do sistema ERP Protheus, segundo o contrato firmado junto a GTI, todo suporte e manutenção é de responsabilidade da fornecedora, TOTVS, permitindo que todas as adequações relacionadas a legislação possam ser customizadas sem ônus adicional à SP Turismo.
		17. Para as demais customizações, a GTI, por intermédio de seus colaboradores da equipe de desenvolvimento e sistemas (CDS), deve realizar a análise e providenciar as pequenas adequações e desenvolvimentos necessários de acordo o processo padrão de desenvolvimento.
			1. Nos casos onde há a necessidade de grades intervenções e/ou a contratação de novos módulos, essa mesma equipe deve cuidar do desenho das especificações necessárias para realização de uma contratação externa.
	2. **Gestão de Acessos**
		1. A GTI deve segregar as funções de seus colaboradores com a finalidade de restringir os poderes concedidos a cada indivíduo de forma que cada um receba conforme sua alçada e apenas as funções que forem pertinentes a cada um.

* 1. **Concessão**
		1. A GTI deve atribuir cada conta ou dispositivo de acesso à computadores, sistemas, bases de dados ou qualquer outro ativo de informação a um responsável, sendo que: os usuários (logins) individuais de funcionários deverão ser de responsabilidade do próprio funcionário; e os usuários (logins) de terceiros devem assinar o Termo de Confidencialidade e Sigilo (vide Anexo II) que garante que a responsabilidade seja transferida para eles.
		2. Em caso de admissão de um colaborador, a equipe da GRH (Gerência de Recursos Humanos) deve realizar o cadastro e criar o usuário através da ferramenta disponibilizada pela GTI na intranet.
		3. Toda ação de criar ou inabilitar um usuário deve ser realizada através dessa ferramenta pela equipe da GRH. A ferramenta deve registrar as interações e enviar os alertas, por e-mail, para a equipe da GTI.
		4. Todas as solicitações de concessão de acessos devem ser realizadas por esta ferramenta, com exceção das permissões de acesso ao ERP que são solicitadas pelos gestores das diversas áreas, com a aceitação do líder de processo de cada segmento do ERP via e-mail ou através de uma CI.
		5. No sistema de chamados, devem ser registradas todas as ocorrências/incidentes de TI para a atendimento de suporte técnico.
	2. **Revogação**
		1. Sob demanda, quando um colaborador é desligado, o responsável da GRH deve realizar a inativação do cadastro do usuário na ferramenta da Intranet, que deve estar parametrizada para comunicar os responsáveis pelos diversos sistemas na TI, que devem providenciar seu bloqueio nas demais ferramentas e ambientes da SP Turismo (Active Directory, E-mail entre outros).
		2. O sistema Protheus deve estar parametrizado para automaticamente inativar o usuário no sistema, sempre que a GRH realizar o seu desligamento do quadro de funcionários ativos.
		3. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.
	3. **Revisão de acessos**
		1. Anualmente, todos os perfis de acessos dos sistemas, aplicativos, rede e bancos de dados devem ser formalizados e revisados periodicamente, assegurando que cada profissional da SP Turismo tenha seus acessos limitados às reais necessidades de suas funções laborais.
		2. Anualmente, o analista de TI deve extrair um relatório contendo todos usuários ativos do sistema Protheus, divididos por área de atuação e enviará para os gestores das áreas de negócio da SP TURIS.
		3. Os gestores devem revisar este relatório, apontando por área de atuação quais os funcionários que devem ou não ter acesso ao sistema Protheus.
		4. Após a revisão, o relatório deve devolvido ao analista de TI responsável pela revisão de acesso, por e-mail, com todos os comentários dos revisores justificando as alterações solicitadas.
		5. A GTI deve executar as solicitações e os documentos devem ser devidamente armazenados, permitindo consultas futuras.
	4. **Revisão de perfis de acessos**
		1. Anualmente, o analista de TI deve extrair do sistema Protheus um relatório contendo quais os tipos de perfis de acessos desenhados para o sistema Protheus.
		2. Para cada um destes perfis, o analista de TI deve destacar quais as funcionalidades dos acessos correspondentes.
		3. Neste relatório, o analista de TI deve registrar seus comentários sobre quais os perfis que deveriam continuar iguais ou quais devem ser alterados.
		4. Após formalização do relatório, este será enviado aos gestores das áreas de negócio da SP Turismo, os quais devem analisar o relatório, verificando possíveis alterações das permissões atribuídas.
		5. Este relatório deve ser devolvido a GTI para que as ações apontadas sejam tomadas.
		6. A GTI deve executar as solicitações e os documentos devem ser devidamente armazenados, permitindo consultas futuras.
	5. **Acessos privilegiados no Sistema Protheus**
		1. Os acessos privilegiados ao sistema Protheus são concedidos via formulário impresso que contém termo de responsabilidade devidamente aprovado pelo Gerente da GTI e assinado pelo colaborador (interno/externo) envolvido.
	6. **Parametrização de senhas**
		1. Para a configuração do ambiente operacional, a GTI deve utilizar uma controladora de domínio baseada no Active Directory e habilitar o requisito de “complexidade de senhas”, cujas premissas básicas para composição da senha pessoal devem ser as seguintes:
			1. Não deve conter partes significativas do nome da conta do usuário ou o nome todo;
			2. Deve ter, pelo menos, seis caracteres de comprimento;
			3. Deve conter caracteres de três das quatro categorias a seguir: Caracteres maiúsculos do inglês (A-Z);
			4. Caracteres minúsculos do inglês (a-z); 10 (dez) dígitos básicos (0-9);
			5. E caracteres não-alfabéticos (por exemplo, !, $, #, %);
		2. Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.
		3. Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.
		4. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação se lhes forem designados.
		5. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.
		6. Após 3 (três) tentativas de acesso, a conta do usuário deve ser bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Coordenadoria de Suporte às Tecnologias da SP Turismo. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).
		7. Os usuários podem alterar a própria senha, e devem ser orientados pela GTI a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha. A periodicidade máxima para troca das senhas é 180 (cento e oitenta) dias, não podendo ser repetidas as 2 (duas) últimas senhas.
		8. Caso o colaborador esqueça sua senha, uma nova senha deve ser requisitada formalmente através de e-mail ou pessoalmente, dirigindo-se a GTI.
	7. **Datacenter**
		1. O datacenter deve estar devidamente localizado em um espaço distinto e qualificado para acomodar toda a infraestrutura de redes e servidores, devendo possuir os seguintes equipamentos de segurança: Acesso físico restrito por meio de chaves; Aparelhos de ar-condicionado dedicados e redundantes; Nobreak para 36 (trinta e seis) horas; Gerador; E extintor de CO2.
		2. O acesso físico deve ser controlado através do uso das chaves, as quais existem duas cópias da porta do Datacenter. Uma das cópias deve ser de posse da GSS (Gerência de Segurança e Serviços Auxiliares) da SP Turismo e a outra, de posse da CRS – Coordenadoria de Redes e Segurança da Informação. O acesso deve ser controlado por câmera de monitoramento 24 (vinte e quatro) horas.
		3. O controle de acesso ao local deve ser realizado pela GSS que mantem cópia das chaves de acesso ao local e registra sua retirada, bem como realiza o monitoramento através das câmeras existentes no local e deve manter ronda física nas imediações, além de um vigilante plantonista.
		4. O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá ser formalizado por e-mail e/ou outro instrumento (CI), bem como assinar o Termo de Responsabilidade.
		5. Caso haja necessidade do acesso, a área requisitante deve solicitar autorização, com antecedência, mínima de 10 (dez) dias, a qualquer colaborador responsável pela administração de liberação de acesso.
		6. O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.
		7. O Datacenter deve ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente deverá ser solicitado a limpeza à área responsável.
		8. A entrada ou retirada de quaisquer equipamentos do Datacenter deve ocorrer mediante o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter.
		9. No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, a revogação dos acessos deve ser providenciada pela GTI.
	8. **Backup**
		1. Os backups dos principais sistemas da SP Turismo devem ser realizados através de um sistema de backup que utiliza um robô automatizado com capacidade para manipulação e armazenamento interno de até 133 (cento e trinta e três) cartuchos de fita LTO 5, sem a intervenção do usuário administrador.
		2. As práticas de backup se fazem necessárias à recuperação de arquivos acidentalmente apagados ou editados erroneamente.
	9. **Modo de realização**
		+ 1. A realização dos backups e sua respectiva restauração devem ser de responsabilidade da CRS (Coordenadoria de Redes e Segurança da Informação), com a seguinte política:
				1. **Segunda-feira** - Período: Noite; Tipo de backup: Cumulative Incremental; Tempo de Retenção: 2 (duas) semanas; e Periodicidade: Todas as semanas.
				2. **Terça-feira** – Período: Noite; Tipo de backup: Diferencial Incremental; Tempo de Retenção: 2 (duas) semanas; e Periodicidade: Todas as semanas.
				3. **Quarta-feira** - Período: Noite; Tipo de backup: Cumulative Incremental; Tempo de Retenção: 2 (duas) semanas; e Periodicidade: Todas as semanas.
				4. **Quinta-feira** – Período: Noite; Tipo de backup: Diferencial Incremental; Tempo de Retenção: 2 (duas) semanas; e Periodicidade: Todas as semanas.
				5. **Sexta-feira** - Período: Noite; Tipo de backup: Full; Tempo de Retenção: 2 (duas) semanas; e Periodicidade: 2 (duas), 3 (três) e 4 (quatro) semanadas.
				6. **Sexta-feira** - Período: Noite; Tipo de backup: Full; Tempo de Retenção: 5 (cinco) anos; e Periodicidade: 1 (uma) semana do mês.
			2. Todos os backups devem ser realizados em fita LTO5, através do robô de backup existente no Datacenter (Centro de Processamento de Dados) da SP Turismo, sendo que o catalogo deverá ser gerado de forma automática pela própria ferramenta de backup.
			3. Há uma VLAN especifica para o estacionamento, garantindo o isolamento desta e das demais redes de dados da SP Turismo visando viabilizar a interligação entre os servidores do SIA, os usuários deste servidor e a infraestrutura do Datacenter.
	10. **Procedimento de restauração dos backups**
		1. A restauração dos arquivos do servidor deve ser realizada, sempre que houver a necessidade ou for demandada pelas áreas de fiscalização.
	11. **Continuidade do negócio**
		1. Com o objetivo de minimizar o impacto sobre a organização, o servidor do novo SIA deve ser instalado em uma unidade IBM Bladecenter com ambiente virtualizado, vmware vsphere com HÁ (High Availability).
	12. **Responsabilidades e Competências**
		1. Colaboradores **em Geral**
			1. Entende-se por colaborador toda e qualquer pessoa física, contratada em qualquer regime, seja ela um funcionário de carreira ou comissionado, de caráter efetivo ou originaria de algum programa de estágio ou outros que descaracterizam um vínculo empregatício direto, mas que lhes obriguem ao cumprimento das normas e condutas exigidas pela São Paulo Turismo S/A., dentro ou fora da instituição, de seus colaboradores.
			2. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar aa São Paulo Turismo S/A ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.
	13. **Colaboradores em Regime de Exceção**
		1. Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto em seu contrato de trabalho quanto a concessão de uso dos serviços de tecnologia da informação.
		2. A concessão poderá ser revogada a qualquer tempo e sem a necessidade de justificativas, sempre que a São Paulo Turismo assim o entender ou se o colaborador que a recebeu não estiver cumprindo as condições definidas no seu “Termo de compromisso e confidencialidade”.
	14. **Gestores de Pessoas ou Processos**
		1. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
		2. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da política de segurança da informação da São Paulo Turismo S/A, seja diretamente ou através da instituição de representante por ele instituído para esse fim.
		3. Exigir de todos os colaboradores sob sua gestão a assinatura do “Termo de Compromisso e Confidencialidade”, caso já não o tenham feito por ocasião de sua contratação através da GRH, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da São Paulo Turismo S/A.
		4. Antes de conceder acesso às informações da instituição e de sua área de negócios, independente de tratar-se de sistema informacional gerido pela área de tecnologia da informação ou outra fonte de dados qualquer que esteja sendo utilizada em sua área, deve certificar-se da existência do ”Termo de Compromisso e Confidencialidade” assinado pelos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato de trabalho existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais ou outra situação qualquer.
		5. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política de segurança da informação, bem como aos termos da norma especifica que vier a ser criada para esse mesmo fim.
	15. **Gerência de Tecnologia da Informação**
		1. A GTI (Gerência de Tecnologia da Informação) é a responsável pela eficácia dos sistemas de monitoramento e controle utilizados na SP Turismo, devendo dar ciência aos demais gestores da SP Turismo sobre possíveis riscos residuais que precisem ser mitigados na forma de regras de conduta interna.
		2. A GTI deve definir quais são os acordos de níveis de serviço (ANS) que serão prestados para cada serviço existente e quais os procedimentos de resposta a incidentes, certificando-se que tais acordos (ANS) atendem às necessidades de seu cliente interno, representado pelas diversas áreas da SP Turismo.
		3. A GTI deve cuidar, ainda, da configuração de todos os equipamentos, ferramentas, sistemas e serviços oferecidos aos colaboradores da SP Turismo, zelando para que todos os controles necessários sejam implementados para fazer cumprir os requerimentos de segurança estabelecidos por esta política de segurança da informação e pelas Normas de Segurança da Informação complementares existentes.
		4. Os ocupantes do cargo de “Analista de Tecnologia da Informação” ou Analista de TI podem, no desempenho de suas atribuições funcionais e pela característica dos privilégios necessários ao desempenho de suas atividades, acessar arquivos e dados de outros usuários nos diversos ambientes funcionais e sistemas da SP Turismo. Entretanto, estabelece esta política de segurança da informação que isso só será licito, quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, a realização de auditorias ou testes nos ambientes.
		5. A GTI deve, na medida em que isso for possível e sem prejuízo das atividades funcionais, segregar as funções de seus colaboradores com a finalidade de restringir ao mínimo os poderes concedidos a cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir logs e trilhas de auditoria das suas próprias ações.
		6. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a São Paulo Turismo S/A.
			1. O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção de cópias e backups, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.
			2. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável, sendo que: Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário; e os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.
			3. Proteger continuamente todos os ativos de informação da SP Turismo contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso ou indesejado.
			4. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da SP Turismo em processos de mudança que envolvam a introdução de novos dispositivos, aplicativos ou aplicações integradas aos já existentes.
			5. Realizar auditorias periódicas de configurações técnicas e análise de riscos.
			6. Garantir, da forma mais rápida possível, mediante solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da SP Turismo (somente a gerência de recursos humanos poderá solicitar), incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da SP Turismo.
			7. Monitorar o ambiente de TI, gerando indicadores e históricos de: Uso da capacidade instalada da rede e dos equipamentos; Tempo de resposta no acesso à internet e aos sistemas críticos da São Paulo Turismo S/A; Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da São Paulo Turismo; Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, etc); e atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).
	16. **Custodiantes da Informação**
		1. Quando ocorrerem movimentações internas de equipamentos, estes deverão ser formatados pelas equipes da GTI antes que sejam disponibilizados a outros usuários na SP Turismo. Essa medida visa resguardar a confidencialidade de informações entre os departamentos, evitando que usuários mal-intencionados possam recuperar informações contidas no equipamento antes da transferência.
		2. Somente os profissionais da GTI estão autorizados a instalar softwares e sistemas nos equipamentos da SP Turismo, bem como somente eles têm autorização para adicionar ou remover tais equipamentos. A nenhum outro colaborador, salvo expressa autorização da GTI, é facultada a execução de atividades que envolvam a manipulação da rede de computadores e seus ativos.
	17. **Coordenadoria de Redes e Segurança da Informação**
		1. Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
		2. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da São Paulo Turismo S/A.
		3. Publicar e promover as versões da política de segurança da informação e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.
		4. Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da São Paulo Turismo S/A, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.
		5. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
		6. Analisar criticamente incidentes em conjunto com o Comitê de Segurança (composto pelos Coordenadores e Gerentes de Redes e Segurança da Informação, Desenvolvimento de Sistemas e Gerência de TI) da Informação.
		7. Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.
		8. Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a São Paulo Turismo S/A.
		9. Buscar alinhamento com as diretrizes corporativas da instituição.
	18. **Regras Gerais**
		1. **Correio Eletrônico**
			1. É terminantemente proibido aos colaboradores o uso do correio eletrônico da São Paulo Turismo para:
			2. Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a
			3. Uso legítimo da instituição;
			4. Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
			5. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a São Paulo Turismo vulnerável a ações civis ou criminais;
			6. Divulgar informações não autorizadas ou cópias de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
			7. Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
			8. Apagar mensagens pertinentes de correio eletrônico quando a São Paulo Turismo S/A promover ou estiver sujeita a algum tipo de investigação ou auditoria.
			9. Produzir, transmitir ou divulgar mensagens que:
				1. Contenham qualquer ato ou forneça orientação que conflite ou contrarie os interesses da São Paulo Turismo;
				2. Contenham ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
				3. Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
				4. Vise obter acesso não autorizado a outro computador, servidor ou rede dentro ou fora da SP Turismo;
				5. Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
				6. Vise burlar qualquer sistema de segurança e segurança da informação interno ou externo;
				7. Pretenda vigiar secretamente ou assediar outro usuário na rede interna ou fora dela;
				8. Vise acessar informações confidenciais sem explícita autorização do proprietário;
				9. Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
				10. Inclua imagens criptografadas ou de qualquer forma mascaradas com a finalidade de ocultar seu verdadeiro conteúdo;
				11. Contenha anexo(s) superior(es) a 15 (quinze) MB para envio (interno e internet) e 15 (quinze) MB para recebimento (internet);
				12. Incorpore em seu conteúdo material considerado impróprio, obsceno ou ilegal;
				13. Possua caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico ou outros proibidos pela legislação;
				14. Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas por lei;
				15. Contenha material de cunho político de qualquer esfera (propaganda política);
				16. Inclua material protegido por direitos autorais sem a permissão do detentor de tais direitos.
			10. Todas as mensagens de correio eletrônico sempre deverão incluir assinatura contendo, no mínimo, informações sobre o nome do colaborador, gerência ou departamento ao qual é vinculado, nome da SP Turismo, Telefones e endereço real de correio eletrônico;
			11. Não está autorizada a criação e veiculação de disclaimer ao final das mensagens enviadas pela ferramenta de correio da SP Turismo. Caso venha futuramente a ser definida essa funcionalidade, será de responsabilidade das equipes da GTI implementa-la, utilizando os recursos computacionais de que dispõem seus servidores.
		2. **Internet**
			1. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a auditoria. A São Paulo Turismo S/A, em total conformidade com as legislações vigentes, reserva-se o direito de monitorar e registrar todos os acessos por ela concedido aos seus colaboradores com a finalidade de fazer cumprir o que assevera a legislação, especialmente falando-se do “Marco Civil da Internet no Brasil” definido pela lei nº 12.965, de 23 de abril de 2014.
			2. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede.
			3. A São Paulo Turismo S/A, ao monitorar sua rede interna, deve garantir a integridade dos dados e programas por ela mantidos. Toda tentativa de alteração dos parâmetros de segurança por qualquer colaborador, sem o devido credenciamento ou autorização para tal, deve ser julgada inadequada e os riscos relacionados a operação serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas pode acarretar as ações administrativas e penalidades cabíveis, inclusive decorrentes de processos civil e criminal se aplicáveis, sendo que nesses casos a SP Turismo cooperará ativamente com as autoridades competentes.
			4. A internet disponibilizada pela SP Turismo aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos de cada setor. É importante observar que é competência do gestor de cada área fiscalizar se é adequado ou não que seus colaboradores utilizem a internet para esses fins, sendo sua a premissa de qualquer tipo de punição nos casos que julgar a existência de abusos.
			5. Entretanto, como é do interesse da São Paulo Turismo S/A que seus colaboradores estejam bem informados, o uso de sites de notícias ou de outros serviços de informação, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais e não perturbe o bom andamento dos trabalhos, gerando conflitos de interesse com os seus objetivos de negócio.
			6. Somente os colaboradores que estão devidamente autorizados a falar em nome da São Paulo Turismo S/A para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.
			7. Apenas os colaboradores autorizados pela instituição podem copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.
			8. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.
			9. Os colaboradores com acesso à internet não podem fazer o download (baixa) de qualquer tipo de programa de computador ou executável de qualquer natureza, exceto quando houver autorização especial para esse fim.
			10. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pelas equipes da GTI.
			11. Os colaboradores não podem em hipótese alguma utilizar os recursos da São Paulo Turismo S/A para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional e passível de penalização.
			12. Como regra geral, materiais de cunho sexual não podem ser exibidos, acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.
			13. Colaboradores com acesso à internet não podem efetuar upload (subida) de qualquer software licenciado pela São Paulo Turismo S/A ou de dados de sua propriedade aos seus parceiros e clientes, sem a expressa autorização do responsável pelos dados e da GTI.
			14. Os colaboradores não podem utilizar os recursos da São Paulo Turismo S/A. para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.
			15. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não são permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) são permitidos apenas a grupos específicos com a devida autorização.
			16. O acesso a serviços de comunicação instantânea (MSN, ICQ, Skype, WhatsApp web e afins) podem ser bloqueados caso o gestor requisite formalmente à GTI.
			17. Da mesma forma, o acesso a redes sociais como o facebook, myspace, flickr, foursquare, google+, Tumblr, tweeter e outras podem ser bloqueadas se solicitado à GTI pelo gestor de cada área.
			18. Não é permitido acesso a sites de proxy ou sua ativação em qualquer dispositivo, exceto pelo pessoal da GTI.
		3. **Computadores e Recursos tecnológicos**
			1. É proibido ao usuário comum realizar qualquer tipo de procedimento para manutenção física ou lógica, instalação, desinstalação, configuração ou modificação dos equipamentos sem o consentimento prévio ou o acompanhamento de um profissional da GTI São Paulo Turismo S/A.
			2. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente podem ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.
			3. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá comunicar imediatamente a área de suporte da GTI através da abertura de um chamado aberto pela intranet.
			4. Arquivos pessoais e não relacionados aos negócios da São Paulo Turismo S/A (fotos, músicas, vídeos, etc). Não devem ser copiados ou movidos para as unidades de rede, pois podem sobrecarregar o armazenamento de nossos servidores. Caso seja identificada a existência desses arquivos, a São Paulo Turismo S/A reserva-se o direito de exclui-los permanentemente de sua infraestrutura de discos e unidades de rede sem prévio aviso.
			5. Documentos imprescindíveis para as atividades dos colaboradores da instituição devem ser salvos nas unidades de rede destinadas a esse fim. Nossos servidores de arquivos garantem a aplicação das políticas de backup e recuperação de dados, necessárias manutenções da integridade. Por outro lado, é terminantemente proibida a gravação e de dados relevantes aos negócios da SP Turismo, exclusivamente nas unidades de disco locais de cada estação de trabalho. Os dados gravados apenas localmente nessas estações de trabalho (por exemplo, no drive C: do computador local), não estão cobertos pela política de backups e segurança da informação e são de total responsabilidade de seus usuários. Caso ocorra alguma falha e sejam perdidos dados ou documentos importantes para a SP Turismo em decorrência dessa prática, considerada irregular por este normativo, o usuário que lhe deu causa será responsabilizado.
			6. No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas, como segue:
				1. Somente a GTI está autorizada a conduzir e instruir os processos de aquisição ou locação de bens, serviços e sistemas de tecnologia da informação, sejam eles para composição e ou recomposição de seu atual parque de informática e ambiente computacional da SP Turismo, ou destinados aos atendimentos de solicitações pontuais emitidas pelas demais áreas da SP Turismo;
				2. Para aquisição ou locação de bens, serviços ou sistemas as áreas interessadas devem encaminhar, através de CI (Correspondência Interna), uma solicitação formal à GTI que, caso exista previsão orçamentária para esse fim, deve conduzir e instruir um processo de compras.
				3. Todos os computadores de uso individual devem ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas devem ser definidas pela GTI da São Paulo Turismo S/A, que terá acesso a elas para manutenção dos equipamentos;
				4. Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;
				5. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um profissional da GTI da São Paulo Turismo S/A ou por terceiros devidamente autorizados pela mesma para esse fim;
				6. Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de TI;
				7. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;
				8. O colaborador deve manter a configuração do equipamento disponibilizado pela São Paulo Turismo S/A, seguindo os devidos controles de segurança exigidos por esta norma, assumindo a responsabilidade como custodiante dessas informações;
				9. Devem ser protegidos por senha (bloqueados), nos termos previstos por esta norma, todos os terminais de computador e impressoras quando não estiverem sendo utilizados;
				10. Todos os recursos tecnológicos adquiridos pela São Paulo Turismo S/A devem ter imediatamente suas senhas padrões (default) alteradas;
				11. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso;
				12. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da São Paulo Turismo S/A;
				13. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
				14. Burlar quaisquer sistemas de segurança;
				15. Acessar informações confidenciais sem explícita autorização do proprietário;
				16. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
				17. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
				18. Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
				19. Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
				20. Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.
		4. **Dispositivos Móveis**
			1. Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua GTI, como: notebooks, smartphones e pendrives.
			2. A São Paulo Turismo S/A, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.
			3. O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na São Paulo Turismo S/A, mesmo depois de terminado o vínculo contratual mantido com a instituição.
			4. Todo colaborador deve realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deve, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.
			5. O suporte técnico aos dispositivos móveis de propriedade da São Paulo Turismo S/A e aos seus usuários deve seguir o mesmo fluxo de suporte contratado pela instituição.
			6. Todo colaborador deve utilizar senhas de bloqueio automático para seu dispositivo móvel.
			7. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da GTI.
			8. O colaborador deve responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da GTI da São Paulo Turismo S/A.
			9. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.
			10. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.
			11. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela São Paulo Turismo S/A, notificar imediatamente seu gestor direto e a GTI. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).
			12. O colaborador deve estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar aa São Paulo Turismo S/A e/ou a terceiros.
			13. O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da São Paulo Turismo S/A deverá submeter previamente tais equipamentos ao processo de autorização da GTI.
			14. Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.
1. **Penalidades**
	1. Todos os colaboradores estarão sujeitos às penalidades das normas disciplinares da SP Turismo, em especial a **NG GRH 07 - Conduta Funcional**, no caso de descumprimento desta Norma.
2. **Legislação básica**
	1. LEI FEDERAL Nº 13.303 - Lei de Responsabilidade das Estatais.
	2. LEI FEDERAL Nº 8.666 - Lei de Licitações e Contratos
	3. LEI FEDERAL Nº 10.520 – Pregão
3. **Anexos**
	1. ANEXO I - Solicitação de Desenvolvimento.
	2. ANEXO II - Termo de Confidencialidade e Sigilo.
4. **Revisões**
	1. Anualmente, as definições e diretrizes desta norma devem ser revisadas e aprovadas pela GTI (Gerência de Tecnologia de Informação) e a CRS (Coordenadoria de Redes e Segurança da Informação).
5. **Histórico de alterações**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revisão** | **Data** | **Alterações** | **Revisores/ Aprovadores** |
| Publicação | Implantação |
|  |  |  |  |  |
| REV. 01  |  |  | Não aplicável | GTI: Nilson Serra |

**ANEXO I**



**Coord. de Desenvolvimento e Sistemas**

**GTI**

**Solicitação de Desenvolvimento – Termo de Início do Projeto**

**Referência:**

**Solicitante:**

**Escopo do projeto:**

Descrever escopo, exemplo:

“Criação de um sistema para controle dos processos envolvidos na comercialização dos serviços de telecomunicações do Parque Anhembi.

O sistema será constituído por dois módulos funcionais integrados na intranet da SP Turismo e utilizará os mecanismos de segurança, autenticação e permissões que essa estrutura proporciona, não sendo possível desassociá-lo de tal infraestrutura.

O sistema será constituído como uma ferramenta de apoio e permitirá ao usuário criar, preencher, receber da internet (através de página web) preenchido, tratar inconsistências, administrar seus status, imprimir, fechar, cancelar e realizar todas os procedimentos necessários para transformar uma “Solicitação” em uma “Ordem de Serviço de instalação” e seu respectivo “Contrato de Prestação de Serviços”.

O sistema NÃO se confunde com um sistema de vendas on-line e tão pouco será responsável por qualquer transação financeira relacionada a venda de tais serviços.

O sistema será responsável, entretanto, por estabelecer os controles necessários ao acompanhamento e registro dessas operações, permitindo que a área de vendas e a área de operações se integrem através de um único ambiente. ”

**Estão contemplados os seguintes entregáveis:**

* Listar
* Listar
* Listar

**Não estão contemplados os seguintes entregáveis:**

* Listar
* Listar
* Listar

Faz parte deste documento a apresentação de requisitos técnicos/funcionalidades, onde aparecem ilustradas as características que este possuirá. Destacamos desse documento a possibilidade de futuramente serem implementadas melhorias e/ou novas funcionalidades ao sistema, não contempladas no presente momento, mas que poderiam constituir uma versão subsequente deste documento.

❖ **Inicio da Análise e Desenvolvimento:** DD/MM/AAAA.

❖ **Data para entrega do sistema de controles:** DD/MM/AAAA.

❖ **Data para entrega do sistema de pagamentos on-line:** DD/MM/AAAA.

**Responsáveis pelo desenvolvimento**

|  |  |
| --- | --- |
|  |  |
| **Nilson A. Serra****Gerente de Tecnologia da Informação** | **XXXXXX****Coordenador de Tecnologia da Informação** |

|  |  |
| --- | --- |
|  |  |
| **XXXXXX****Área Requisitante** |  |

**ANEXO II**



**TERMO​ ​DE​ ​CONFIDENCIALIDADE​ ​E​ ​SIGILO**

São Paulo Turismo S/A.

Eu **NOME COMPLETO**, **ESTADO CIVIL**​, inscrito no CPF sob o nº **XXX.XXX.XXX-XX**​, abaixo firmado, assumo o compromisso de manter confidencialidade e sigilo sobre todas as informações técnicas e outras a que tiver acesso dentro da São Paulo Turismo S/A.

Por este termo de confidencialidade e sigilo comprometo-me:

1. A não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;

2. A não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso;

3. A não me apropriar, para uso próprio ou de outrem, do material confidencial e/ou sigiloso da tecnologia que venha a ser disponibilizada para execução de minhas atividades;

4. A não repassar o conhecimento das informações confidenciais, responsabilizando-me por todas as pessoas que vierem a ter acesso às informações, por meu intermédio, e obrigando-me, assim, a ressarcir a ocorrência de qualquer dano e / ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Confidencial significará toda informação revelada através da apresentação da tecnologia, a respeito de, ou, associada com a Avaliação, sob a forma escrita, verbal ou por quaisquer outros meios.

Informação Confidencial inclui, mas não se limita, à informação relativa às operações, processos, planos ou intenções, informações sobre produção, instalações, equipamentos, segredos de negócio, segredo de fábrica, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, produtos, amostras, diagramas, desenhos de esquema industrial, patentes, oportunidades de mercado e questões relativas a negócios revelados da tecnologia supra mencionada.

Avaliação significará todas e quaisquer discussões, conversações ou negociações entre, ou com as partes, de alguma forma relacionada ou associada aos serviços objeto do contrato Nº.**XXX/XXXX**.

A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, terá a validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo.

Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

São Paulo, **XX** de **MÊS** de 20**XX**.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**NOME COMPLETO ​ ​|​ ​ EMPRESA TERCEIRA**

**RG: ​ ​XXX.XXX.XXX-X**