

TIVIT	POLÍTICA	Código	Revisão
		SEG-POL-001-018	2
	Política de Segurança da Informação para Fornecedores	Classificação da Informação	Página
		Público	1 de 8

ÍNDICE

1. OBJETIVO.....	2
2. APLICAÇÃO E ÁREAS ENVOLVIDAS	2
3. VERSÃO E APROVAÇÃO DO DOCUMENTO	2
4. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO	3
4.1. <i>Código de Conduta</i>	<i>3</i>
4.2. <i>Documentação Normativa de Segurança da Informação da TIVIT.....</i>	<i>4</i>
5. RESPONSABILIDADES GERAIS DO FORNECEDOR TIVIT	4
5.1. <i>Identificação de Desvios / Riscos.....</i>	<i>5</i>
5.2. <i>Comunicação de incidentes de segurança da informação</i>	<i>5</i>
6. RESPONSABILIDADES ESPECÍFICAS.....	5
6.1. <i>Gestão de ativos.....</i>	<i>5</i>
6.2. <i>Controle de acesso físico e lógico.....</i>	<i>6</i>
6.3. <i>Delimitação de perímetro e proteção de segurança física.....</i>	<i>6</i>
6.4. <i>Uso aceitável de ativos e recursos.....</i>	<i>6</i>
6.5. <i>Análise e garantias de segurança em sistemas de informação fornecidos.....</i>	<i>6</i>
6.6. <i>Recursos Humanos, Interações e Comunicações.....</i>	<i>7</i>
6.7. <i>Planos de Continuidade, Desastre ou situação de emergência.....</i>	<i>7</i>
6.8. <i>Requisitos Legais e Regulamentares adicionais</i>	<i>7</i>
6.9. <i>Criptografia, Privacidade e Monitoramento</i>	<i>7</i>
6.10. <i>Sub-contratação.....</i>	<i>8</i>

Cópias impressas não autorizadas

TIVIT	POLÍTICA	Código	Revisão
		SEG-POL-001-018	2
	Política de Segurança da Informação para Fornecedores	Classificação da Informação	Página
		Público	2 de 8

1. OBJETIVO


O objetivo desta política de segurança da informação é orientar Fornecedores TIVIT sobre as diretrizes de segurança da informação em vigor, assim como descrever sua participação e responsabilidade no cumprimento das metas e estratégias de excelência estabelecidas pela TIVIT como fornecedora de produtos e serviços de tecnologia da informação. As instruções e regras aqui descritas devem ser seguidas para garantir, de forma consistente e eficiente, a proteção das informações disponibilizadas pela TIVIT, assim como o uso apropriado de recursos tecnológicos, ambientes e dependências acessados pelos Fornecedores TIVIT em razão da prestação de serviços, garantindo a correta custódia e evitando ameaças deliberadas ou acidentais.

2. APLICAÇÃO E ÁREAS ENVOLVIDAS

Fornecedores e parceiros TIVIT.

3. VERSÃO E APROVAÇÃO DO DOCUMENTO

Ação	Detalhe	Versão	Responsável	Aprovador	Data
Criação do documento	Versão inicial do documento	1	Marcelo Carvalho	Grace Meirelles	01/04/2020

	POLÍTICA	Código	Revisão
		SEG-POL-001-018	2
	Política de Segurança da Informação para Fornecedores	Classificação da Informação	Página
		Público	3 de 8

4. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Todos os Fornecedores TIVIT devem estar comprometidos quanto à observação da política de segurança de informação da TIVIT não fornecendo ou apropriando-se indevidamente de recursos de informações, utilizando sistemas e recursos tecnológicos somente de acordo com autorizações e instruções especificadas pela TIVIT, zelando e preservando ativos. Devem estar, ainda, imbuídos de manter e preservar os princípios básicos de segurança da informação:

- **Confidencialidade** – O Fornecedor TIVIT deve contribuir para a manutenção do sigilo e restrição de acesso das informações compartilhadas ou acessadas em razão do exercício de sua função e serviço contratado. Todas as informações compartilhadas ou acessíveis ao Fornecedor TIVIT devem ser tratadas como sigilosas e pertencentes à TIVIT.
- **Integridade** – O Fornecedor TIVIT compromete-se com o uso adequado e autorizado de ativos TIVIT, inclusive informações. Não é permitida a manipulação ou edição de ativos de informações fora do seu escopo de trabalho ou limitações impostas por procedimentos ou controles de acesso em sistemas de informação.
- **Disponibilidade** – O Fornecedor TIVIT preza pela preservação dos ambientes e recursos tecnológicos TIVIT de seu fornecimento ou suporte, de forma a favorecer a continuidade e oferta ininterrupta de serviços.

É considerado incidente de segurança da informação envolvendo Fornecedores TIVIT, qualquer desrespeito aos princípios de segurança da informação e, em especial, a violação de dados: caracterizada pela violação de segurança que leva à destruição acidental ou ilícita, à perda ou à divulgação não autorizada, acesso a dados protegidos transmitidos ou armazenados, e transformação ou processamento não permitidos.


Os incidentes de segurança originados por Fornecedores TIVIT podem ocasionar investigações que resultam em sanções, punições e responsabilizações legais, assim como cancelamentos de contrato e dever de indenizar.

4.1. Código de Conduta

É responsabilidade de todos os colaboradores, Fornecedores e parceiros TIVIT, a conduta correta e ética, obedecendo os preceitos de respeito às pessoas e preservação da imagem da TIVIT e seu compromisso com segurança da informação.

Espera-se dos Fornecedores TIVIT um comportamento ético e de elevado moral, respeito e a observância às leis vigentes assim como dos regulamentos TIVIT, incluindo:

- Exercer o trabalho profissional com responsabilidade, dedicação, honestidade e justiça, buscando sempre a melhor solução;

	POLÍTICA	Código	Revisão
		SEG-POL-001-018	2
	Política de Segurança da Informação para Fornecedores	Classificação da Informação	Página
		Público	4 de 8

- Esforçar-se para adquirir continuamente competências técnicas e profissionais, mantendo-se sempre atualizado com os avanços da profissão e especialidades;
- Atuar dentro dos limites de sua competência profissional;
- Guardar sigilo profissional das informações que tiver acesso em razão do exercício de suas atividades contratadas;
- Atender às expectativas de confiança depositadas pela TIVIT, acessando e utilizando recursos e informações apenas no limite da necessidade para realização de seu trabalho e autorização concedida;
- Pautar sua relação com colegas nos princípios de consideração, respeito e solidariedade, assim como conduzir as atividades profissionais, que envolvam interação ou contribuição em grupo, sem discriminação de qualquer tipo, seja de cor, sexo, nacionalidade, idade, religião, estado civil ou qualquer outra condição humana;
- Honrar compromissos e prazos estabelecidos;
- Não praticar atos deliberados que possam comprometer segurança, privacidade ou que atentem para diminuição ou anulação de controles e proteções de segurança estabelecidos pela TIVIT.


4.2. Documentação Normativa de Segurança da Informação da TIVIT

Para suportar o Sistema de Gerenciamento de Segurança da Informação TIVIT (SGSI), aderente à norma nacional ABNT NBR ISO/IEC 27001:2013 para implementar, monitorar e melhorar os controles e indicadores de eficiência e eficácia do processo que garante a segurança da informação na TIVIT, diversos documentos, procedimentos e instruções são publicadas e atualizadas constantemente. É responsabilidade do Fornecedor TIVIT a observância destas normativas, ainda que não explicitamente contidas nesta política, específica. Para isso, o Fornecedor TIVIT deve buscar, sempre que não encontrar orientação suficiente neste documento, instruções específicas junto à TIVIT e complementar o entendimento dos requisitos de segurança da informação, quando necessário.

O Fornecedor TIVIT deve manter-se informado dos requisitos e normas TIVIT que regulam sua atuação junto à TIVIT, assim como das atualizações destas documentações.

5. RESPONSABILIDADES GERAIS DO FORNECEDOR TIVIT

Todos os Fornecedores TIVIT devem seguir as orientações gerais de segurança da informação e contribuir para a identificação de ameaças e riscos à operação TIVIT.

	POLÍTICA	Código	Revisão
		SEG-POL-001-018	2
	Política de Segurança da Informação para Fornecedores	Classificação da Informação	Página
		Público	5 de 8

5.1. Identificação de Desvios / Riscos

Todo e qualquer impeditivo da prestação de serviço na forma acordada deverá ser reportado a TIVIT, para que seu impacto seja analisado e comunicado, internamente, minimizando impactos a reputação e imagem da TIVIT e/ou sua atuação específica contratada.

5.2. Comunicação de incidentes de segurança da informação

Os Fornecedores TIVIT são parte integrante do fluxo de comunicação de eventos de segurança que possam interferir negativamente em sua atuação contratada ou indicar comportamento anormal de recursos de TI em uso. Tais eventos podem vir a ser classificados como incidentes de segurança da informação pela TIVIT e tratados adequadamente para garantir a integridade e qualidade da infraestrutura de TI TIVIT.


Todo comportamento anormal de serviços de rede e sistemas de informação, percebidos pelo Fornecedor TIVIT, deve ser reportado para: abuse@tivit.com ou csirt@tivit.com

6. RESPONSABILIDADES ESPECÍFICAS

Os Fornecedores TIVIT devem seguir as orientações específicas de segurança da informação, quando aplicável.

6.1. Gestão de ativos

- Os Fornecedores TIVIT devem observar regras para o uso de equipamentos computacionais autorizados pela TIVIT em ambientes de trabalho, tais como aparelhos celulares, tablets, computadores pessoais e wearables. Todos os equipamentos computacionais trazidos para o ambiente de trabalho, nas dependências da TIVIT, devem ser declarados.
- O Fornecedor TIVIT que usar equipamentos computacionais de propriedade da TIVIT deve utilizá-lo apenas para os fins descritos na contratação específica, sendo responsável pela manutenção do estado de conservação do equipamento e sua devolução imediata ao setor responsável, assim que rescindida ou encerrada sua contratação junto à TIVIT.
- A necessidade de guarda ou transporte de equipamentos computacionais pelo Fornecedor TIVIT deve ser expressamente autorizada pela TIVIT. Apenas locais de guarda e trânsito destes equipamentos especificados na autorização concedida podem ser utilizados pelo Fornecedor TIVIT.
- Apenas mídias de guarda e transporte de ativos de informação expressamente autorizadas pela TIVIT podem ser utilizadas pelo Fornecedor TIVIT.
- Não é permitida a guarda de ativos de informação TIVIT pelo Fornecedor TIVIT após o encerramento da atividade contratada, salvo determinação contrária estabelecida em contrato.

	POLÍTICA	Código	Revisão
		SEG-POL-001-018	2
	Política de Segurança da Informação para Fornecedores	Classificação da Informação	Página
		Público	6 de 8

6.2. Controle de acesso físico e lógico

- Os Fornecedores TIVIT devem portar identificação clara e visível (crachá / etiqueta) ou oferecer documentação de identificação pessoal sempre que solicitado.
- Os Fornecedores TIVIT devem utilizar identificação e autenticação de usuários de sistema concedidos formalmente pela TIVIT para realização de suas atividades, informando de erros ou acessos que não correspondam ou excedam ao escopo de sua atuação contratada.
- As credenciais de acesso a sistemas disponibilizadas para Fornecedores TIVIT são de uso intransferível.
- Sistemas de informação fornecidos por Fornecedores TIVIT, para uso de colaboradores TIVIT, devem oferecer autenticação segura e prover meios de rastreabilidade de ações realizadas. A disponibilização ou integração de tais sistemas deve, preferencialmente, utilizar múltiplos fatores (Strong authentication) e, minimamente, conectar-se aos controladores TIVIT por meio de Serviços de Federação do Active Directory (autenticação moderna do Azure AD) para autenticação de usuários.

6.3. Delimitação de perímetro e proteção de segurança física


- Os Fornecedores TIVIT devem atuar e transitar apenas em locais expressamente autorizados e relacionados a sua atuação contratada.

6.4. Uso aceitável de ativos e recursos

- Os Fornecedores TIVIT devem utilizar ativos de informação apenas para o propósito relacionado a sua atuação contratada.
- Os Fornecedores TIVIT não podem reconfigurar ou alterar capacidades e restrições definidas em equipamentos e recursos tecnológicos de propriedade TIVIT. Equipamentos e recursos tecnológicos de posse ou propriedade do Fornecedor TIVIT, utilizados em sua atuação contratada não devem oferecer riscos e vulnerabilidades. O uso de tais equipamentos pode estar sujeito a inspeção e avaliação da TIVIT a qualquer tempo e, inclusive, a proibição de uso.

6.5. Análise e garantias de segurança em sistemas de informação fornecidos

- Sistemas de informação fornecidos por Fornecedores TIVIT, para uso de colaboradores TIVIT e / ou seus clientes, devem oferecer garantias de segurança de informação aplicada. Certificados de análises de segurança vigentes, realizadas por entidades terceiras e independentes competentes, devem ser apresentados sempre que solicitado. Adicionalmente, a TIVIT reserva-se o direito de realizar análises de segurança (scan de vulnerabilidades, testes de penetração ou outro) para manutenção desta garantia de segurança da informação nestes sistemas.

	POLÍTICA	Código	Revisão
		SEG-POL-001-018	2
	Política de Segurança da Informação para Fornecedores	Classificação da Informação	Página
		Público	7 de 8

6.6. Recursos Humanos, Interações e Comunicações

- Os Fornecedores TIVIT devem utilizar apenas recursos humanos (colaboradores) expressamente declarados e autorizados para a prestação das atividades contratadas (mesmo em atividades executadas fora das dependências TIVIT).
- As interações entre o Fornecedor TIVIT e a TIVIT devem ser realizadas pelos meios e mídias autorizados pela TIVIT.
- A comunicação e envio de informações deve ocorrer de forma segura, observando os protocolos e aplicativos de comunicação autorizados pela TIVIT.

6.7. Planos de Continuidade, Desastre ou situação de emergência

- Quando acionados em cenário de contingência, ativação de planos de continuidade e/ou recuperação de desastres, os Fornecedores TIVIT responsáveis por ações de emergência, devem priorizar as ações conforme nível de prioridade classificado pela TIVIT, respeitando os Acordos de Nível de Serviço (ANS) definidos em contrato.
- Caso definido em contrato, os Fornecedores TIVIT que suportam áreas críticas de negócio, devem oferecer, regularmente, resultados de testes de execução de planos de continuidade e/ou recuperação de desastres relacionados aos produtos e serviços escopo do contrato, de forma a demonstrar atendimento ao processo, entregáveis e tempos acordados com a TIVIT.
- Todas as ações de emergência executadas com a participação do Fornecedor TIVIT devem obedecer aos princípios de segurança da informação estabelecidos pela TIVIT.

6.8. Requisitos Legais e Regulamentares adicionais

- Todas as imposições de segurança, adicionais a esta política, determinadas por requisitos Legais ou Regulamentos Setoriais aos quais a TIVIT estiver submetida, geram obrigação de cumprimento solidário do Fornecedor TIVIT, limitado à sua atuação contratada.
- Caso o Fornecedor TIVIT armazene dados da TIVIT ou de seus Clientes fora do território nacional, deverá informar a TIVIT do país de armazenamento. A mudança de armazenamento para qualquer outro país diferente do informado inicialmente deve ser previamente consultada e autorizada pela TIVIT.

6.9. Criptografia, Privacidade e Monitoramento

- O Fornecedor TIVIT que manusear dados pessoais em detrimento de sua atividade contratada é responsável pela garantia de que esses dados sejam gerenciados de acordo com todas as normas de Privacidade e Proteção de Dados Pessoais aplicáveis.
- Todas as informações confidenciais, com acesso concedido ao Fornecedor TIVIT, devem obedecer aos princípios de segurança e gestão de chaves estabelecidos pela TIVIT. Não é permitido ao Fornecedor TIVIT alterar permissões ou interferir na gestão de acesso a informações de propriedade da TIVIT.

TIVIT	POLÍTICA	Código	Revisão
		SEG-POL-001-018	2
	Política de Segurança da Informação para Fornecedores	Classificação da Informação	Página
		Público	8 de 8

- A TIVIT se reserva ao direito de monitorar e controlar ações de credenciais utilizadas por Fornecedores TIVIT, assim como inspecionar o conteúdo de mensagens e comunicações efetuadas por meio do uso da rede de computadores sob responsabilidade da TIVIT.

6.10. Sub-contratação

- O Fornecedor TIVIT que optar pela sub-contratação de parte ou todo o escopo de serviços, deve obter anuência prévia da TIVIT para tal.
- Caso a sub-contratação seja aprovada pela TIVIT, é responsabilidade do Fornecedor TIVIT a garantia do conhecimento e cumprimento de todas as diretrizes aqui dispostas pelos sub-contratados.

Cópias impressas não são autorizadas