

	<p>POLÍTICA DE FORNECEDORES</p>	<p>CÓDIGO : PUB-PL09 VERSÃO : 01</p>
---	---------------------------------	--

ELABORADOR/ APROVADOR		
RESPONSÁVEL		DATA
ELABORADOR	Luc Salmon	25/06/2021
APROVADOR	Henri Le Rasle	26/06/2021

### Histórico de revisão

Versão	Date	Descrição
1.0	05/06/2021	Versão inicial

## 1.Introdução

Esta política gera a relação e interação da Ecritel com seus fornecedores.

## 2.Listagem de Fornecedores Relevantes / Críticos

**Criticidade alta:** Fornecedores de criticidade alta fazem armazenamento e processamento de dados da ecritel ou de seus clientes. Devem seguir padrões altos de segurança da informação (nível ISO27001).

**Criticidade Média:** Fornecedores de criticidade média podem ter acessos a alguns dados sensíveis da Ecritel sem impacto direto às operações. Devem aceitar termos de confidencialidade e não divulgação da Ecritel.

**Criticidade Baixa:** Fornecedores que lidam com tarefas que não teriam impacto imediato ou grande nas atividades da ecritel. Devem aceitar termos de confidencialidade e não divulgação da Ecritel.

Nome	Descrição Produto/ Serviço	Criticidade	Análise de criticidade
Provedor de serviços cloud de comunicação e gerenciamento de documentações.	Serviços digitais de armazenamento: Email, google drive etc..	Alta*	Comunicações e documentos/ arquivos sensíveis da Ecritel estão armazenados na infraestrutura do fornecedor. Pelo tamanho/perfil da empresa, a Ecritel confia nas políticas estabelecidas pelo fornecedor. A Ecritel tem conferido a política de segurança / privacidade do fornecedor para assegurar a sua adequação às necessidades.
Datacenter	Hospedagem de servidores	Alta*	O Datacenter hospeda toda infraestrutura da ecritel e seus clientes. Para garantir sua segurança Ecritel tem um acordo NDA com o datacenter e verifica o status de sua certificação 27001 anualmente.



Datacenter Digital	Hospedagem de servidores	Alta*	Dados de sites e clientes da Eritel estão armazenados na infraestrutura do fornecedor. Pelo tamanho/perfil da empresa, a Eritel confia nas políticas estabelecidas pelo fornecedor. A Eritel tem conferido a política de segurança / privacidade do fornecedor para assegurar a sua adequação às necessidades.
Empresa do RH		Média	A empresa trata dos salários de colaboradores Eritel
Empresa Contabil	Contabilidade	Média	A Empresa tem acesso a fluxos financeiros da Eritel
Fornecedores de materiais	Equipamentos de produção, materiais de consumo e outros	Baixa	Sem acesso a dados sensíveis ou internos da Eritel

\*Fornecedores marcados não estão sujeitos a todos os controles de aderência à política de fornecedores

### 3.Regras para Fornecedores

Os únicos fornecedores que têm acesso a dados internos Eritel são os que fornecem serviços financeiros, legais, e contábeis. Porém eles têm acesso restrito apenas à informação enviada para eles, não têm acessos a sistemas internos ou espaços físicos ecritel.

Fornecedores de baixa e média criticidade precisam assinar um NDA "INT-F08- Termo de Confidencialidade" para garantir sua confidencialidade.

Provedores de *hospedagem de servidores* precisam manter seu status com certificação 27001, e



os procedimentos de controle de acesso.

Para os outros fornecedores, como são baixo-risco e baixa criticidade, não são necessárias outras medidas de segurança ou controle.

O padrão da ecritel para transferência de dados com partes externas e usando e-mail e telefonemas/call para podermos proteger a integridade, confidencialidade e disponibilidade das informações.

Quaisquer mudanças feitas por fornecedores que possam ter um impacto nos serviços dos mesmos, da ecritel, ou na segurança da informação devem ser previamente comunicados para que a Ecritel avalie os possíveis impactos e tome ações necessárias.

## 1 Acordo Fornecedor

Esta carta formaliza as expectativas da Ecritel em relação aos seus fornecedores e subcontratados no que diz respeito à segurança da informação e descreve as regras relativas às intervenções de fornecedores terceiros ou prestadores de serviços na Ecritel.

Ao ler esta carta, o fornecedor ou subcontratado concorda em cumprir estritamente o conteúdo.

Todas as obrigações em termos de segurança da informação (incluindo confidencialidade e restituição de dados), mesmo após a vigência do contrato entre a Ecritel e seu Fornecedor.

### 1.1 Objetivos

Ser fornecedor ou provedor da Ecritel significa:

- Conduzir os negócios de acordo com as regras éticas
- Compromisso de respeitar todas as leis e regulamentos em vigor
- Compromisso em entregar produtos e serviços que atendam aos padrões de qualidade e segurança exigidos pela legislação vigente

- Atuar conjuntamente para a melhoria contínua de seus produtos e serviços
- Comprometer-se com os princípios descritos abaixo e concordar em ser avaliado por um terceiro em sua inscrição
- Adotando os princípios deste Estatuto nas relações com seus próprios Fornecedores

## 1.2 Conformidade

A Eritel espera que o fornecedor ou subcontratados cumpram todas as leis e regulamentos aplicáveis, especialmente no que diz respeito aos pilares detalhados neste documento, e se esforça para cumprir os padrões internacionais e da indústria e as melhores práticas.

## 1.3 Escopo

O reconhecimento desta carta é uma condição importante em qualquer contrato com a Eritel. Ao aceitar o que se refere este regulamento, o Fornecedor ou subcontratado compromete-se a garantir que todas as suas atividades cumpram o disposto neste certificado.

Qualquer violação significativa dos princípios estabelecidos nesta carta pode resultar, dependendo de sua importância, em uma lista para baixo do Fornecedor ou subcontratado.

# 2 ENVOLVIMENTO DO FORNECEDOR

## 2.1 Respeito pela carta ética

### *Respeito à ética e lealdade*

O Fornecedor compromete-se a:

- Conduza os negócios com honestidade
- Luta contra todas as formas de corrupção (ativa ou passiva)
- Proibir estritamente qualquer pagamento pessoal, suborno ou suborno
- Preste atenção especial ao modesto valor de face dos presentes ou privilégios concedidos aos funcionários da Eritel

Esses presentes ou privilégios devem:

- Seja aceitável de uma perspectiva legal
- Combine uma ocasião específica (final do ano ...)



### *Respeito à legalidade*

O Fornecedor compromete-se a cumprir todas as leis e regulamentos aplicáveis:

- Respeito pelos direitos humanos
- A luta contra todas as formas de discriminação
- A luta contra o trabalho forçado e a proibição do trabalho infantil
- Proteção da saúde e segurança
- O respeito ao meio ambiente
- A luta contra todas as formas de corrupção e contra a concorrência desleal
- Prevenção de conflitos de interesse
- O direito de propriedade e a proteção de informações confidenciais
- Níveis de remuneração e horas de trabalho
- A prática de diálogo e consulta com os funcionários e o direito à negociação coletiva

## **2.2 Respeito à confidencialidade e segurança**

### *Garantir a confidencialidade dos dados e das partes interessadas*

- Qualquer informação comunicada pela Ecritel deve ser considerada confidencial em relação a outros clientes atuais e futuros do fornecedor e seus próprios fornecedores, prestadores de serviços ou subcontratados
- Qualquer informação relativa à relação comercial entre o fornecedor e a Ecritel deve ser utilizada apenas no contexto estrito desta relação e não pode, em caso algum, ser comunicada a terceiros sem o consentimento prévio por escrito da Ecritel
- Cada fornecedor deve garantir, quando apropriado, a implementação adequada e o respeito estrito dos acordos de confidencialidade por seus funcionários e qualquer parte interessada envolvida

O provedor está comprometido com a confidencialidade das informações às quais sua equipe pode ter acesso. Cada pessoa em questão deve ter assinado um acordo de confidencialidade.

O fornecedor está comprometido com as ações que sua equipe pode realizar. Cada pessoa interessada deve ter assinado um termo de confidencialidade individual limitando suas ações à única necessidade de intervenções. Este compromisso pode ser agrupado com o anterior.

O fornecedor deve, no mínimo, sensibilizar as pessoas autorizadas, para garantir o acesso (físico e lógico) às estações de intervenção remotas e no local e disponibilizar, se necessário, as estações de intervenção e os meios de segurança associados.

### *Regras que regem as intervenções no local ou remotas*

O fornecedor assume um compromisso de:

- Não tomar cópia dos documentos e suportes de informação que lhe forem confiados, exceto os necessários à execução deste serviço previsto no contrato, sendo necessária a concordância prévia do capitão do arquivo
- Não use os documentos e informações processados para finalidades diferentes das especificadas neste contrato
- Não divulgue esses documentos ou informações a outras pessoas, sejam elas privadas ou públicas, físicas ou jurídicas
- Tomar todas as medidas para evitar qualquer uso indevido ou uso fraudulento de arquivos de computador durante a execução do contrato
- Tomar todas as medidas de segurança, inclusive físicas, para garantir a preservação e integridade dos documentos e informações processadas durante a vigência deste contrato

### *Regras que regem as intervenções no local*

Cada fornecedor deve conhecer e aplicar as políticas, procedimentos e normas de segurança quando intervém nas instalações do estabelecimento ou num dos centros de dados da Eritel.

As regras de acesso são as seguintes:

- Qualquer intervenção é necessariamente planeada através de um processo que envolve um pedido de autorização prévia do apoio ao cliente.
- Durante o acesso no local, o pessoal do fornecedor é acompanhado no local em áreas sensíveis por pessoal autorizado da equipe técnica da Eritel.
- O fornecedor se compromete a respeitar os procedimentos e processos definidos pela instituição para acessar as informações de que necessita para o desempenho de suas funções. Ele também concorda em não tentar substituir os controles de acesso e controles existentes por nenhum motivo.

### *Regras que regem o acesso remoto como parte da manutenção*

- O provedor deve garantir a segurança de sua plataforma de intervenção remota, pontos de vista de acesso, proteção de dados e software
- O provedor deve restringir o acesso lógico das estações de resposta apenas a pessoas autorizadas
- O provedor deve restringir o acesso físico das estações de resposta apenas a pessoas autorizadas



- O fornecedor deve ser capaz de determinar em todas as circunstâncias a identidade de qualquer pessoa que se conecte ou tenha feito logon em sua plataforma e garanta a rastreabilidade
- O fornecedor deve implementar meios e procedimentos de acordo com as regras , para combater incidentes que possam afetar a segurança da informação ou a própria intervenção
  - o Combate a incidentes de segurança no ambiente humano, organizacional, técnico ou físico do provedor
  - o Luta contra a propagação de código malicioso ou incidentes de segurança da plataforma do fornecedor ou por meio de trocas eletrônicas como parte da entrega
  - o A luta contra códigos maliciosos no software transmitido como parte do serviço ou em sua atualização e contra a exploração de vulnerabilidades conhecidas nestes elementos
- O fornecedor deve implementar um dispositivo de gerenciamento de configuração para controlar o acesso aos componentes produzidos ou fornecidos para manutenção de software (código-fonte, código executável, documentação, dados de teste, etc.)
- O provedor deve garantir que, após cada intervenção remota, os dados residuais (arquivos temporários ou áreas de RAM) sejam apagados da plataforma
- Uma intervenção só é considerada concluída quando o objetivo da intervenção é alcançado (resolução de um incidente, atualização de um componente ...) ou que o responsável e o fornecedor declarem de comum acordo que o objetivo não é alcançável

## 2.3 Relatório de qualquer violação

O fornecedor é obrigado a relatar qualquer suspeita de violação de segurança, regras, leis e do Código. Ele entrará em contato com a pessoa de contato da Ecritel ou usará o email: [seguranca@ecritel.com.br](mailto:seguranca@ecritel.com.br)