



## POLÍTICA DE PRIVACIDADE INTERNA

### GRUPO YAMAM

#### Sumário

<b>1. PROPÓSITO, ESCOPO E USUÁRIOS .....</b>	<b>2</b>
<b>2. DOCUMENTOS DE REFERÊNCIA.....</b>	<b>2</b>
<b>3. DEFINIÇÕES.....</b>	<b>3</b>
<b>4. PRINCÍPIOS BÁSICOS RELATIVOS AO TRATAMENTO DE DADOS PESSOAIS .....</b>	<b>4</b>
<b>5. DOS DADOS PESSOAIS .....</b>	<b>5</b>
<b>6. POLÍTICA DE MESA LIMPA .....</b>	<b>7</b>
<b>7. USO DE E-MAIL CORPORATIVO .....</b>	<b>8</b>
<b>8. RESPOSTA A INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS .....</b>	<b>10</b>
<b>9. SANÇÕES DISCIPLINARES .....</b>	<b>10</b>
<b>10. DA SEGURANÇA DA INFORMAÇÃO .....</b>	<b>11</b>
<b>11. VALIDADE E GERENCIAMENTO DE DOCUMENTOS .....</b>	<b>12</b>



## **1. Propósito, Escopo e Usuários**

A YAMAM tem o compromisso de proteger a privacidade dos dados pessoais de seus funcionários, clientes, parceiros de negócios e outras pessoas. Desta forma, a Cisco implementou um programa global de privacidade e proteção de dados para estabelecer e manter padrões elevados para coletar, usar, divulgar, armazenar, proteger, acessar, transferir ou processar dados pessoais. Esta política global de privacidade e proteção de dados pessoais é a base do programa e descreve a abordagem adotada pela Cisco ao processar dados pessoais em todo o mundo.

Os usuários deste documento são todos os colaboradores, permanentes ou temporários, inclusive prestadores de serviços, e todos os contratados que trabalham em nome da Empresa.

O cumprimento dessa Política poderá ser auditado.

## **2. Documentos de Referência**

- Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- Decreto nº 7.724, de 16 de maio de 2012: Regulamenta a Lei no 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que dispõe sobre o acesso a informações previsto na Constituição.
- Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
- Atribuições do Encarregado de Proteção de Dados (DPO)
- Procedimento pedido de acesso dos titulares de dados
- Termo aditivo de contrato de trabalho para LGPD
- Termos de eliminação, retenção, consentimento e confidencialidade do colaborador
- Política de uso de internet
- Código de conduta de uso de mensageiro instantâneo
- Política de incidentes e plano de respostas



### 3. Definições

Para os fins desta política de Privacidade Interna, consideram-se:

**Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

**Dados pessoais:** quaisquer informações relativas a uma pessoa singular identificada ou identificável (“**titular dos dados**”); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular;

**Dados pessoais sensíveis:** dados pessoais que são, por sua natureza, particularmente sensíveis em relação aos direitos e liberdades fundamentais e que, por isso, merecem proteção específica, pois o contexto de seu tratamento pode criar riscos significativos aos direitos e liberdades fundamentais. Esses dados pessoais incluem dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

**Controlador:** a pessoa física ou jurídica de direito privado, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.

**Operador:** a pessoa física de direito privado, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do Controlador.

**Tratamento:** toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

**Compartilhamento de dados:** comunicação, difusão, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, com autorização específica;

**Confidencialidade:** garantia de que a informação é acessível somente por pessoas autorizadas;

**Internet:** sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

**Sítios e aplicativos:** instrumentos por meio dos quais o usuário acessa os serviços e conteúdos disponibilizados;



**Terceiro:** pessoa ou entidade que não participa diretamente em um contrato, em um ato jurídico ou em um negócio, ou que, para além das partes envolvidas, pode ter interesse num processo jurídico;

**Segurança da informação:** conjunto de práticas e métodos voltados para a preservação da confidencialidade, integridade e disponibilidade da informação.

#### 4. Princípios básicos relativos ao tratamento de dados pessoais

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

**Finalidade:** a realização do tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao(à) titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

**Adequação:** a compatibilidade do tratamento deve ocorrer conforme as finalidades informadas ao(à) titular, de acordo com o contexto do tratamento;

**Necessidade:** o tratamento deve se limitar à realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

**Livre acesso:** é a garantia dada aos(às) titulares de consulta livre, de forma facilitada e gratuita, à forma e à duração do tratamento, bem como à integridade de seus dados pessoais;

**Qualidade dos dados:** é a garantia dada aos(às) titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

**Transparência:** é a garantia dada aos(às) titulares de que terão informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

**Segurança:** trata-se da utilização de medidas técnicas e administrativas qualificadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

**Prevenção:** compreende a adoção de medidas para prevenir a ocorrência de danos por causa do tratamento de dados pessoais;

**Não discriminação:** sustenta que o tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos;



**Responsabilização e prestação de contas:** demonstração, pelo Controlador ou pelo Operador, de todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.

## **5. Dos Dados Pessoais**

Os Dados Pessoais pertencem à pessoa natural a quem se referem as informações, na condição de Titulares de Dados Pessoais. Todos seus direitos são previstos e assegurados pela Lei Geral de Proteção de Dados Pessoais e deverão ser observados pela YAMAM durante o Tratamento destes dados.

Os Dados Pessoais deverão sempre serem classificados como: de uso interno, restrito e confidenciais. Além de conhecer essa Política, é obrigação do colaborador ter ciência de todos os termos e políticas mencionadas neste documento (item 2).

### **a) Coleta de Dados Pessoais**

A YAMAM deve se esforçar para coletar a menor quantidade de dados pessoais possível. Se os dados pessoais forem coletados de terceiros, o Encarregado de Proteção de Dados deve garantir que os dados pessoais são coletados legalmente.

### **b) Utilização, Guarda e Descarte de Documentos**

Documentos que contenham Informações classificadas como uso interno, restrita ou confidencial ou com Dados Pessoais não podem ficar expostos na estação de trabalho, em impressoras, scanner, telas de computadores, áreas comuns, locais de trânsito de pessoas, refeitório e nas salas de reunião.

Sob nenhuma hipótese documentos de nenhum tipo que contenham Dados Pessoais poderão ser utilizados como rascunho.

Referidos documentos devem ser acondicionados em armários de acesso controlado, sua destruição, quando for o caso, deverá ser feita por meio de triturador de papel. Nenhuma das Informações restritas ou confidenciais ou Dados Pessoais podem ser repassadas para terceiros sem consentimento formalizado da YAMAM.

Deve-se observar a exigência e o prazo legal definido em tabela vigente à época, para manutenção dos documentos produzidos em razão de suas atividades. Decorrido o prazo para armazenamento, os documentos devem ser destruídos antes de descartados, mediante autorização prévia do gestor responsável.



E, se for este o caso, a empresa de guarda externa deverá emitir Certificado ou Declaração de Destruição Segura dos documentos indicados pela YAMAM.

#### **c) Recebimento de Currículos**

A coleta de currículos (*curriculum vitae*) deverá ocorrer somente quando houver processo de seleção aberto. Contudo, caso haja o recebimento de currículo fora de processo de seleção, deverá ser armazenado nas condições especificadas nos padrões de privacidade da YAMAM.

O prazo para armazenamento de currículos deverá ser de até 6 (seis) meses, contado da data do recebimento, devendo haver um controle interno efetivo sobre o prazo. Documentos físicos (recebidos em papel) deverão ser digitalizados, armazenados em sistema ou rede e descartados por meio de trituradora ou equivalente ou, ainda, compilados (com as informações necessárias à eventual contratação) em sistema. É vedado o armazenamento em arquivos físicos ou *hardwares*.

O candidato deverá ser informado sobre o período de armazenamento e retenção dos dados e orientado sobre como agir para retificar e atualizar seus dados, de forma simples e didática, por e-mail ou aviso no site. Todo o processo de tratamento de dados por este meio deverá obedecer todas as demais orientações sobre uso, retenção e eliminação de dados.

#### **d) Uso, retenção e eliminação**

As finalidades, métodos, limitação de armazenamento e período de retenção de dados pessoais devem ser consistentes com as informações contidas nos termos e avisos disponibilizados ao titular de dados pessoais. A YAMAM deve manter a exatidão, integridade, confidencialidade e relevância dos dados pessoais com base na finalidade do tratamento. Mecanismos de segurança adequados projetados para proteger dados pessoais devem ser usados para evitar que dados pessoais sejam roubados, mal utilizados ou utilizados de maneira desconforme à finalidade, além de serem evitadas violações de dados pessoais.

Em relação aos documentos que contenham Dados Pessoais, estes deverão ser tratados de forma adequada e limitada pelo período em que se fizerem necessários para cumprimento do propósito especificado ao Titular de Dados Pessoais. A YAMAM reserva-se o direito de manter armazenado uma cópia de todos os processos realizados para seus clientes, incluindo os Dados Pessoais, devendo zelar integralmente pela sua guarda e sigilo, nos termos da legislação vigente e, ainda, considerando-se os prazos prescricionais dos atos praticados durante a vigência do contrato firmado ou consentido entre as partes.



**e) Divulgação para Terceiros**

Sempre que a YAMAM usa um fornecedor ou parceiro de negócios para tratar dados pessoais em seu nome, O Encarregado de Proteção de Dados deve garantir que este operador forneça medidas de segurança para proteger dados pessoais apropriados aos riscos associados.

A YAMAM deve exigir contratualmente que o fornecedor ou parceiro de negócios forneça o mesmo nível de proteção de dados. O fornecedor ou parceiro de negócios deve apenas tratar dados pessoais para cumprir suas obrigações contratuais com a YAMAM ou sob as instruções dela e não para quaisquer outros fins. Quando a YAMAM trata dados pessoais em conjunto com terceiros independentes, deve especificar explicitamente suas respectivas responsabilidades e as de terceiros no contrato relevante ou em qualquer outro documento juridicamente vinculante.

**f) Direitos de Acesso por Titulares de Dados**

Ao atuar como um controlador de dados, é responsável por fornecer aos titulares de dados um mecanismo de acesso razoável para permitir que eles acessem seus dados pessoais, e deve permitir que eles atualizem, retifiquem, apaguem ou transmitam seus Dados Pessoais, se apropriado ou exigido por lei.

**6. Política da Mesa Limpa**

Deve ser seguido o princípio estabelecido na Norma ABNT NBR/ISO/IEC 27001, que tem como objetivo a redução dos riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente.

A política de “Mesa Limpa/Tela Limpa” busca resguardar a YAMAM, bem como o próprio usuário contra o acesso não autorizado a Informações e Dados Pessoais. Assim, sinteticamente, entre outros:

- a)** Papéis, anotações e lembretes devem ser mantidos fora da superfície da mesa (mesa limpa);
- b)** Informações restritas ou confidenciais e/ou Dados Pessoais devem ser trancadas em local separado (idealmente em um arquivo, armário ou gaveteiro) quando não necessárias, especialmente quando o ambiente ficar vazio, como no final do expediente;
- c)** Computadores e notebooks não devem ser deixados autenticados/registrados quando não houver um colaborador junto e devem ser protegidos por senhas e outros controles quando não estiverem em uso (tela limpa). Assim, o colaborador deverá ter por hábito utilizar sempre o Ctrl + Alt + Delete + Bloquear sempre que for deixar o equipamento, ainda que por alguns instantes;
- d)** Utilização de protetor de tela que solicite uma senha para acesso deve ser sempre usado;



- e) Informações restritas ou confidenciais e/ou Dados Pessoais, quando impressos, devem ser retiradas da impressora imediatamente pelo colaborador que solicitou a impressão;
- f) Ao final do dia, ou no caso de ausência prolongada, a mesa de trabalho deve ser limpa;
- e
- g) Todos os documentos e meios eletrônicos, no final do dia de trabalho, devem ser devidamente guardados/organizados, com proteção adequada.

## **7. Uso de E-mail Corporativo**

Os serviços de correio eletrônico (e-mail) são oferecidos como um recurso profissional pela YAMAM para seus colaboradores no cumprimento de seus objetivos nas áreas de atuação.

O uso pessoal não é permitido, assim, assuntos pessoais deverão ser tratados em e-mail pessoal apenas.

Cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal. Deve ser considerado que o correio eletrônico é inerentemente uma forma insegura de comunicação, não garantindo sigilo ou entrega.

A YAMAM poderá fornecer recursos adequados para melhorar o nível de segurança no uso do correio eletrônico, como, por exemplo, chaves de criptografia e assinatura digital.

O acesso às mensagens nos servidores de correio eletrônico deve ser feito usando protocolos seguros.

Os colaboradores e parceiros com acesso, aos serviços de mensagem eletrônica disponibilizados pela YAMAM, deverão estar cientes de que as mensagens trocadas no ambiente de e-mail corporativo poderão ser auditadas a qualquer tempo pela YAMAM e devem observar o seguinte:

- a) Todos os usuários dos ativos de Informações de propriedade da YAMAM, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse da empresa, mantendo uma conduta ética e profissional;
- b) Todas as contas de e-mail terão uma titularidade, sendo o usuário titular o responsável direto pelas mensagens enviadas por intermédio do seu endereço de e-mail;
- c) Todos os e-mails enviados/recebidos deverão ser excluídos após 6 (seis) meses da data do recebimento. Caso seja necessária a guarda de informações contidas em determinada mensagem, o colaborador deverá utilizar o ambiente adequado para o armazenamento, utilizando-se do sistema/rede, respeitada a finalidade;
- d) Os usuários poderão ser titulares de uma única caixa postal individual no servidor de e-mail, com direitos de envio/recebimento de mensagens, via Intranet e Internet;
- e) Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens;
- f) O usuário deve utilizar o e-mail de forma adequada e diligente;



- g)** É vedado o disparo de Ordens de Serviço (OS) em massa, devendo o endereçamento se ater à pessoa/departamento que efetivamente deva receber o e-mail;
- h)** O envio de documentos e informações pessoais só poderá ser realizado por e-mail em caráter excepcional, sendo vedada a prática como hábito ou praxe;
- i)** É vedado o envio, armazenamento ou manuseio de material que caracterize a divulgação, incentivo ou prática de atos que:
- Contrariem o disposto na legislação vigente, ética, moral e de ordem pública;
  - Sejam proibidos pela presente Política, lesivos aos direitos e interesses da YAMAM ou de terceiros;
  - De qualquer forma, possam danificar, inutilizar, invadir, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;
  - Promovam ameaças, difamação ou assédio a outras pessoas;
  - Conttenham conteúdo considerado impróprio, obsceno ou ilegal;
  - Sejam de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
  - Conttenham a prática de qualquer tipo de discriminação relativa a raça, sexo, credo religioso, incapacidade física ou mental ou outras situações protegidas;
  - Caracterizem violação de direito autoral garantido por lei.
- j)** É vedada ainda a utilização do e-mail, nas situações abaixo:
- Acesso não autorizado à caixa postal de outro usuário;
  - Uso para atividades com fins comerciais ou políticos e o uso extensivo para assuntos pessoais ou privados;
  - Envio de mensagens do tipo “corrente” e “spam”;
  - Envio intencional de mensagens que conttenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;
  - Utilização de listas e/ou caderno de endereços da YAMAM para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;
  - Envio de qualquer mensagem que torne a empresa vulnerável a ações civis ou criminais;
  - Exclusão de mensagens relacionadas às atividades profissionais, quando a YAMAM ou pessoas a ele relacionadas estiverem sujeitos a algum tipo de investigação.



A YAMAM possui instrumentos para o bloqueio ou cópia de mensagens de maneira a subsidiar processos internos de sindicância ou para atendimento de ordem judicial. O bloqueio poderá ser aplicado a recepção de mensagens provenientes de alguns locais, comerciais ou não, em caso de inconveniência e/ou possível ameaça contida em mensagens indesejáveis.

Os usuários devem utilizar em sua assinatura padrão texto que identifica os requisitos de Segurança da Informação relacionados a confidencialidade da troca de informações, servindo como instrução a terceiros que recebam mensagens provenientes da YAMAM.

“AVISO: A informação contida neste e-mail, bem como em qualquer de seus anexos, é CONFIDENCIAL e destinada ao uso exclusivo do (s) destinatário (s) acima referido (s), podendo conter informações sigilosas e/ou legalmente protegidas. Caso você não seja o destinatário desta mensagem, informamos que qualquer divulgação, distribuição ou cópia deste e-mail e/ou de qualquer de seus anexos é absolutamente proibida. Solicitamos que o remetente seja comunicado imediatamente, respondendo esta mensagem, e que o original desta mensagem e de seus anexos, bem como toda e qualquer cópia e/ou impressão realizada a partir destes, sejam permanentemente apagados e/ou destruídos. A YAMAM se reserva ao direito de manter as informações recebidas de acordo com relevância dos dados pessoais fornecidos, sempre observada a finalidade do tratamento.”

## **8. Resposta a incidentes de violação de dados pessoais**

Quando a Empresa souber de um incidente de segurança ou de uma violação concreta de dados pessoais, o Encarregado de Proteção de Dados deve realizar uma investigação interna e tomar as medidas corretivas apropriadas em tempo hábil.

Quando houver qualquer risco para os direitos e liberdades dos titulares de dados, a Empresa deve notificar a Autoridade nacional de Proteção de Dados – ANPD - sem atrasos indevidos, no prazo de 48 horas, de acordo com a Política de Resposta a Incidentes da YAMAM.

## **9. Sanções disciplinares**

Qualquer colaborador que viole esta Política estará sujeito a uma ação disciplinar. O colaborador também poderá estar sujeito a responsabilidades civis ou criminais se sua conduta violar leis ou regulamentos.



## **10. Da Segurança da Informação**

A equipe responsável pela Segurança da Informação deverá promover a elaboração de um documento abordando questões relacionadas a backup, controle de acessos e logins, utilização da rede, entre outros.

## **11. Validade e gerenciamento de documentos**

Este documento é válido a partir de **01/08/2021**.

O Comitê de Privacidade e o Encarregado de Proteção de Dados deverão revisar e, se necessário, atualizar este documento pelo menos uma vez por ano.

São Paulo, 01 de agosto de 2021

---

**Claudia Renata de C. Visetti**  
Presidente do Comitê



Versão:	01.2021
Data da versão:	01/08/2021
Aprovado por:	
Nível de confidencialidade:	

#### Histórico de Alterações

Data	Versão	Criado por	Descrição da mudança