POLÍTICA DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO

03/07/2023

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

Introdução

Esta Política de Segurança da Tecnologia da Informação visa a atender as diretrizes mínimas com relação ao tratamento de dados pessoais, de acordo com a Lei número 13.709/2018, alterada pela Lei Geral de Proteção de Dados 13.853/2019, no âmbito das atividades exercidas pela REVAL, sem prejuízo de outras providências que se façam necessárias para a integral conformidade com a LGPD.

Para fins legais de auditoria, a empresa se reserva ao direito de realizar investigações em qualquer dos equipamentos que integrem a rede local da REVAL, bem como monitorar e verificar envio de *e-mails* e acesso à *Internet*.

A presente Política deverá ser revista, pelo menos a cada dois anos, levando-se em consideração, dentre outras questões, mudanças regulatórias ou eventuais deficiências encontradas. E a qualquer momento, sempre que o Encarregado de Dados (Gerente Administrativo e Supervisora da Qualidade) ou o Comitê gestor de proteção de dados pessoais entender necessário.

Betim, 03 de julho de 2023.

Eunides Santos	Bruno Gontijo	Valdemar Gontijo
Analista de TI	**Gerente Administrativo**	**Diretor**

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

Sumário

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

1) Objetivo

O objetivo da Política de Segurança da Tecnologia da Informação é manter o nível de segurança da organização em um patamar definido como adequado pela mesma e garantir que as diretrizes explicitadas nesta Política sejam praticadas. Isto é, realizado através da implementação de controles que visam a garantir a confidencialidade, a integridade e a disponibilidade das informações.

A Política de Segurança da Tecnologia da Informação tem como princípios assegurar a:

- **Identificação:** garantir que qualquer indivíduo seja identificado unívoco e inequivocamente.
- **Autenticação:** garantir que a identidade das pessoas ou recurso seja expressamente comprovada.
- **Autorização:** garantir que somente as pessoas e recursos permitidos tenham acesso aos ativos.
- **Confidencialidade:** garantir que as informações sejam acessadas apenas por aqueles expressamente autorizados.
- **Integridade:** preservar a integridade das pessoas e ativos, salvaguardando-os contra ações não autorizadas e garantindo que todas as informações estejam exatas e completas durante a sua criação, uso, guarda e destruição.
- **Disponibilidade:** garantir que os usuários, quando devidamente autorizados, tenham acesso às informações e instalações sempre que necessitarem.

Para atingir este objetivo, a REVAL estabelece a presente Política como um dos pilares de sua estratégia de segurança, que deve ser seguida e implementada para garantir que os ativos sejam protegidos de acordo com a sua importância estratégica para a organização.

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

Ressalta-se que, primordialmente, todos os que necessitem ter acesso aos recursos de rede da REVAL, deverão, como requisito básico, assinar "Termo de Responsabilidade", comprometendo-se à estrita observância e obediência às condições e requisitos básicos para o acesso aos recursos computacionais da REVAL, cujo descumprimento incorrerá nas penalidades cabíveis de acordo com a infração cometida e penalidades previstas em legislação competente. O referido "Termo de Responsabilidade", bem como esta Política de Segurança da Tecnologia da Informação, estarão disponíveis para *download* na área de SGQ destinada e deverão ser disponibilizados a todos os usuários da rede REVAL.

2) Verificação de conformidade

Para garantir as regras que serão mencionadas, a REVAL utiliza os seguintes meios:

a) sistemas que podem monitorar e gerar relatórios do uso de *Internet* através da rede e das estações de trabalho da empresa;
b) sistemas de proteção da rede interna para garantir a integridade dos dados e acessos, incluindo *firewall* com filtro de aplicações, *proxy* com filtro de sites não permitidos ou com controle de horário, sistema de detecção de intrusos, entre outros;
c) sistemas de inspeção de arquivos armazenados na rede, área de transferência ou nas áreas privadas da rede, visando a assegurar o rígido cumprimento desta política;
e) sistema de *e-mails* com segurança de Anti-Spam para evitar chegada de *e-mails* não permitidos ou com vírus;
d) inventário de *software* e *hardware* para monitorar as estações de trabalho e identificar o uso ou a modificação não autorizada das características da estação.

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

As atitudes consideradas violação a esta política encontram-se divididas nos seguintes tópicos:

- utilização da rede corporativa;
- utilização do *e-mail Outlook*;
- utilização do acesso à *Internet*;
- proteção contra vírus e ataques;
- *backup* e restauração de sistemas;
- notificações e incidentes de segurança.

2.1) Utilização da rede Corporativa

Esse tópico visa a definir as normas de utilização da rede da REVAL. Para assegurar o *backup* dos dados, os arquivos relacionados às atividades profissionais dos colaboradores da REVAL devem ser salvos na rede corporativa (cada departamento/usuário deve assegurar que já possui pasta na rede corporativa) e não gravar dados na raiz do computador.

Os arquivos a serem transferidos entre os colabores da REVAL devem ser salvos na unidade pública (z:\transfere$). Esta pasta, assim como todos os recursos de tecnologia, somente deve ser utilizada para fins estritamente profissionais, sendo o conteúdo, periodicamente, excluído pelo Departamento de Tecnologia da Informação.

a) É de responsabilidade do usuário manter o sigilo das suas senhas de acesso à rede e aos sistemas.
b) Todo usuário é responsável pelos atos executados com seu identificador (login), que é único e requer senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia. O usuário deve assegurar a confidencialidade de sua senha de acesso – ela não pode ser compartilhada, sendo de uso pessoal, intransferível e deverá ser trocada periodicamente.
c) Não é permitido material de natureza pornográfica e de caráter sexual, pornografia infantil (pedofilia), apologia ao terrorismo ou às drogas.

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

d) Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário.

e) Não é permitida a conexão de dispositivos não autorizados na rede local, principalmente, equipamentos de rede sem fio como *Access Points*, *wireless*, *bluetooth*, ou qualquer outra solução que estabeleça conexão simultânea com a rede local.

f) A inclusão de novos equipamentos na rede interna deverá ser executada pelo Técnico destinado a estes fins, instalação de S.O. básico com suas respectivas atualizações e instalação dos demais softwares necessários às funções a que se destina, e, somente mediante prévia requisição e autorização. As credenciais de administrador do equipamento deverão ficar sob a guarda e responsabilidade do técnico que efetua tais instalações.

g) Não é permitido o uso de qualquer tipo de programa não relacionado às funções e atividades pertinentes ao trabalho desenvolvido para a REVAL.

h) Instalações e/ou remoções de *softwares* deverão ser efetuadas somente pelo Técnico destinado a estes fins.

i) Antes de ausentar-se do seu local de trabalho, o usuário deverá efetuar o *logout/logoff* da rede ou bloqueio da estação de trabalho através de senha.

j) É de responsabilidade do usuário colocar em pasta específica e orientada para que seja feito o *backup* dos seus arquivos importantes para o desempenho das funções sob sua responsabilidade. É necessário solicitar ao Técnico área reservada no Servidor para estes fins, para evitar perda de informações.

2.2) Utilização do *e-mail* e *Outlook*

Esse tópico visa a definir as normas de utilização do *e-mail* e *Outlook*. O uso do e-mail corporativo (*Outlook*), é a única ferramenta de e-mail autorizada dentro da REVAL. Seu uso está baseado nas premissas de civilidade, eficiência e rapidez, sempre objetivando aumentar a produtividade nos trabalhos diários. Seguem as regras de uso:

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

a) O *e-mail Outlook* deve ser de uso restrito para as atividades relacionadas ao desempenho das funções do usuário. Deve ser usado apenas para propósitos relacionados com o negócio (ex.: para comunicar-se com clientes e distribuidores e para juntar informações comerciais úteis.

b) Para fins legais de auditoria, a empresa se reserva ao direito de realizar investigações nas caixas postais do *e-mail.*

c) O usuário é o único responsável pelo conteúdo das transmissões feitas através do *e-mail* a partir de sua senha ou conta.

d) As mensagens de e-mail são confidenciais, somente podendo ser acessadas pelo remetente e seu destinatário. É proibida a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela.

e) É proibido o assédio ou perturbação de outrem, seja através de linguagem utilizada, frequência ou tamanho das mensagens.

f) É proibido o envio de grande quantidade de mensagens de *e-mail* ("junk mail" ou "spam") que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, envio de arquivos muito grandes que contenham fotos e outros. Na dúvida, consulte o Técnico responsável.

g) É proibido reenviar ou, de qualquer forma, propagar mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens. Exemplo: mensagens de “corrente”.

h) O usuário deverá ficar atento ao tipo de *e-mail* que recebe para evitar abrir *e-mails* com vírus. Em caso de dúvida encaminhe o *e-mail* para o responsável técnico para análise (informatica@revalbombas.com.br).

i) É proibido forjar qualquer das informações do cabeçalho do remetente.
O colaborador não poderá obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados ao serviço.

j) Não é permitida a utilização do *webmail*. O acesso será liberado somente com autorização da área de TI.

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

2.3) Utilização do acesso à *Internet*

Esse tópico visa a definir as normas de utilização da *Internet*. Alguns sites (páginas da Internet) contêm ou distribuem material que não são apropriados a um ambiente de trabalho. Os colaboradores não devem acessar tais sites, distribuir ou obter material similar através da *Internet*. Os acessos a sites podem estar sendo monitorados a qualquer tempo.

a) É proibido utilizar os recursos da empresa para fazer o *download* ou distribuição de *software* ou dados não legalizados.
b) É proibida a divulgação de informações confidenciais da empresa em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, ficando aquele que assim proceder, sujeito às penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei.
c) A *Internet* poderá ser utilizada para atividades não relacionadas com as atividades de trabalho no horário de almoço, desde que dentro das regras de uso definidas nesta política.
d) É proibida a veiculação de pornografia por *e-mail*, seja ele *Outlook* (durante o horário de trabalho), ou pessoal (no horário do almoço).
e) É proibido acesso a sites de natureza pornográfica e de caráter sexual, pornografia infantil (pedofilia), apologia ao terrorismo, às drogas, à violência ou ao racismo. As tentativas de acesso serão gravadas. A insistência será vista como tentativas de conduta que visa a burlar a Política de Segurança da Tecnologia da Informação.
f) Os usuários da área técnica, por força de suas funções e conhecimento, devidamente autorizados, se reservam ao direito de efetuar suas próprias instalações, bem como, permanecer com a guarda e o uso oportuno das credenciais de administrador. Tais usuários poderão efetuar *download* de *softwares* necessários à execução de suas atribuições, devendo providenciar, quando for o caso, a regularização da licença e o registro desses de forma a evitar possíveis penalidades à REVAL.

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

g) Caso a empresa julgue necessário, haverá bloqueios de acesso a arquivos e sites que comprometam o uso de banda da rede, o desempenho e produtividade das atividades do empregado, bem como, que exponham a rede a riscos de segurança.

h) É proibida a utilização de meios para tentar burlar as políticas de bloqueios automaticamente aplicadas pela REVAL. Tais meios envolvem *web-proxy* e tunelamentos criptografados. Apenas em casos restritos, com a devida autorização e quando se fizer necessário para execução de suas atividades, é que o usuário poderá se utilizar de tais recursos.

i) Haverá geração de relatórios dos sites acessados por usuário para verificação da adequação à política vigente;

j) Não será permitido o uso abusivo de comunicação instantânea (*WhatsApp*, *Skype*, *Gtalk* e afins) de forma que venha a impactar na produtividade das atividades da REVAL. O tempo de uso desses recursos será monitorado e relatórios serão enviados para a Diretoria para as devidas providências.

k) Não será permitida a utilização de *softwares peer-to-peer* (P2P), tais como *Emule, Kazaa, Morpheus, Torrents* e afins.

l) A utilização de serviços de redes sociais, só poderá ser realizada, com prévia autorização da Diretoria, desde que sejam serviços pertinentes às atividades da REVAL.

2.4) Proteção contra vírus e ataques

O vírus de computador é um programa desenhado para causar perda ou alteração de dados do computador.

Todo equipamento deve ter um programa antivírus instalado, sendo os softwares antivírus com atualização diária, automática e obrigatoriamente.

O usuário deve efetuar regularmente a busca por vírus em seu computador. Caso seja encontrado vírus deverá consultar a equipe de suporte técnico para obter orientações.

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

Caso o usuário receba algum *e-mail* alertando sobre vírus, não deverá passá-lo a outras pessoas, pois a maioria desses alertas é falso. Permanecendo a dúvida, deverá entrar em contato com a equipe de suporte técnico para maiores explicações.

2.5) *Backup* e restauração de sistemas

A importância dos backups na administração de sistemas nunca pode ser minimizada.

Sem eles, muitos dados são simplesmente irrecuperáveis, caso sejam perdidos devido a uma falha acidental ou a um incidente de segurança.

Cada usuário tem um diretório no servidor de arquivos. Todos os documentos que digam respeito ao negócio deverão ser salvos neste diretório.

O backup de dados pessoais nas estações de trabalho é de total responsabilidade do usuário.

O backup dos servidores é executado pela equipe de Tecnologia da Informação seguindo os procedimentos definidos pela área.

2.6) Notificação e incidentes de Segurança

Qualquer suspeita de incidente de segurança deverá ser informada à Gerência de Tecnologia. Nenhum usuário deverá investigar por conta própria, nem atuar para se defender do ataque. As ações deverão ser executadas pelo setor de Tecnologia da Informação, que está capacitado para conter as exposições, analisar os impactos e conduzir investigações, coletando evidências para possíveis ações jurídicas. A Gerência de Tecnologia está capacitada para conter as exposições, analisar os impactos e conduzir investigações, coletando evidências para possíveis ações jurídicas.

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br

3) Penalidades

O não cumprimento pelo usuário das normas ora estabelecidas neste documento Política de Segurança da Tecnologia da Informação, seja isolada ou cumulativamente, poderá ensejar, de acordo com a infração cometida, as seguintes punições:

a) **Comunicação de descumprimento:** será encaminhado ao funcionário, por *e-mail*, notificação informando o descumprimento da norma, com a indicação precisa da violação praticada e, em caso de reincidência, será enviada também, uma cópia para a Diretoria.
b) **Advertência ou suspensão:** a pena de advertência ou suspensão será aplicada nos casos legais.
c) **Demissão por justa causa:** a pena de demissão por justa causa será aplicada nas hipóteses previstas no artigo 482 e parágrafo único da Consolidação das Leis do Trabalho - decreto-lei N.º 5.452, de 1º de maio de 1943.

Aos funcionários terceirizados, será solicitado à empresa prestadora da respectiva mão-de-obra, o afastamento definitivo do funcionário, podendo a REVAL solicitar a substituição deste ou até mesmo, rescindir o contrato de prestação de serviço, conforme cláusulas contratuais pré-estabelecidas.

Rua Toyota, 175 | Jardim Piemont | Betim / MG | Cep: 32.689-354
Tel: +55 31 3529-7600 | Fax: +55 31 3597-0346 | reval@revalbombas.com.br | www.revalbombas.com.br