

OBJETIVA



Política de Segurança da Informação



Maceió,
Agosto de 2024.

Qualificação

Razão social: Objetiva DISTRIBUIDORA LTDA

CNPJ: 02.865.831/0001-51

Endereço: V SECUNDARIA 3 (DISTRITO INDUSTRIAL), TABULEIRO DO MARTINS

E-mail: dpo@verdesmares.net

1. Objetivo da política



- 1.1. Com o advento da Lei Geral de Proteção de Dados (LGPD), a Objetiva investiu na segurança da informação para proporcionar uma experiência segura e transparente de tratamento de dados para clientes, prestadores de serviço, fornecedores e empregados. A política de segurança da informação formaliza um guia de melhores práticas para reafirmar e padronizar a segurança da informação dentro da instituição. Esta política passou por revisões envolvendo as lideranças e houve aprovação do corpo gestor da organização.

2. Escopo



- 1.1. A Política de Segurança da Informação deve ser seguida por todos, incluindo, mas não se limitando a: empregados, prestadores de serviços temporários, prestadores de serviço integrais, terceirizados, executivos, acionistas, auditores, consultores, fornecedores e parceiros de negócio que estejam a serviço da Objetiva em qualquer etapa do processo.

3. Responsabilidades de segurança da informação

DPO



- Prestar esclarecimentos para os titulares de dados sobre tratamento de dados pessoais e direitos previstos na LGPD;
- Prestar esclarecimentos para a ANPD;
- Auditar a conformidade da operação com a PSI;
- Monitorar a tabela de temporalidade e o descarte adequado das informações;
- Orientar e esclarecer sobre melhores práticas de segurança da informação e proteção de dados.

Fornecedores



- Ler, assimilar e praticar a PSI durante o período integral durante a prestação de serviços em nome da Objetiva;
- Manter o sigilo das informações e dados pessoais da VM e/ou informações que estejam provisoriamente sobre sua posse;
- Garantir a segurança no processamento de dados da Objetiva feitos em sistemas terceiros.
- Comunicar a VM em caráter urgente, no caso de um incidente de segurança da informação.

Membro do comitê



- Assessorar o DPO sobre decisões que possam impactar a confidencialidade, disponibilidade e integridade de dados pessoais e dados internos e confidenciais;

Empregados e prestadores de serviço



- Ler, assimilar e praticar a PSI durante o período integral de trabalho em nome da Objetiva;
- Manter sigilo das informações e dados pessoais da Objetiva e/ou informações que estejam provisoriamente sobre sua posse;
- Acionar o Encarregado da proteção de dados no caso de dúvidas sobre a segurança das informações e proteção de dados pessoais.



6. Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD) está em vigor no Brasil e existe para proteger dados pessoais. Para atender tal requisito, a Objetiva elegeu um DPO (Encarregado da Proteção de Dados) para esclarecer sobre melhores práticas de proteção de dados e para controlar situações internas que possam estar em desconformidade com a legislação. Caso precise falar com o DPO, utilize o endereço eletrônico abaixo:



dpo@objetivadistribuidora.com.br

6.1 Orientações gerais sobre a LGPD

- Todo e qualquer dado pessoal processado pela Objetiva deve ser utilizado exclusivamente para a finalidade informada no momento da coleta;
- Não faça o compartilhamento de dados pessoais (nome, telefone, e-mail, etc.) sem consultar o Encarregado da Proteção de Dados (DPO);
- Não registre dados pessoais em dispositivos particulares, sempre utilize os equipamentos e armazenamento providos pela Objetiva;
- Caso receba algum questionamento sobre o cumprimento da Lei Geral de Proteção de Dados (LGPD), redirecione o questionamento para o Encarregado da Proteção de Dados (DPO) através do endereço informado acima.



4. Classificação da informação

4.1 Tipos de Informação

A Objetiva trata diversos tipos de informações durante seu ciclo de vida operacional. A classificação dessas informações permite a escolha correta dos métodos de segurança que serão aplicados.



- **Público:** Informações sem restrição de compartilhamento.
- **Interno:** Informações que devem ser mantidas internamente e controladas de acordo com o nível de acesso cedido ao colaborador ou fornecedor.
- **Confidencial:** Informações com acesso restrito ao grupo selecionado para o acesso. O sigilo deve ser mantido durante todo o ciclo de vida da informação.

4.2 Esquema de cores

A Objetiva adotará um esquema de cores para garantir a fácil identificação dos tipos de informação:



- **Verde:** Informações públicas.
- **Amarelo:** Informações internas.
- **Vermelho:** Informações confidenciais.

4.3 Rótulo da informação

Todas as informações físicas devem ser rotuladas com sua data de expiração e a correta classificação de cores. Caso a informação esteja em ambiente digital, a seguinte nomenclatura será utilizada nos títulos dos documentos:

- **ANO - P - Título do Documento:** Informações públicas.
- **ANO - I - Título do Documento:** Informações internas.
- **ANO - C - Título do Documento:** Informações confidenciais.

5. Diretrizes gerais de segurança da informação

5.1 Uso de senhas

- A troca de senhas para acesso aos computadores deverá ser alterada a cada 45 dias;
- Não registre as senhas em locais de fácil acesso e/ou em locais que possam ser acessados por outras pessoas;
- Respeite o tempo de vida útil da senha e troque-a quando necessário;
- A senha de usuário é INTRANSFERÍVEL e não deve ser compartilhada nem mesmo com o setor de tecnologia da informação;
- Caso desconfie que sua senha não está mais segura, sinta-se à vontade para alterá-la, mesmo antes do prazo de validade pré-determinado;
- Os sistemas de informação da Objetiva registram logs de atividade de usuário e, portanto, auditorias sobre a utilização das senhas para realização de ações poderão ser realizadas pelo setor de tecnologia da informação;



5.2 Comunicação no ambiente digital



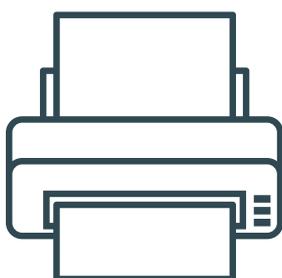
- O e-mail corporativo deve ser usado exclusivamente para fins profissionais e que tenham relevância para a Objetiva;
- Desconfie de e-mails ou mensagens instantâneas com assuntos estranhos ao seu conhecimento;
- Antes de enviar uma mensagem, verifique se todos os destinatários precisam receber a informação. Evite o envio de dados pessoais e confidenciais para remetentes não desejados;
- Utilize apenas as ferramentas de comunicação homologadas pelo setor de tecnologia da informação da Objetiva, seguindo as seguintes instruções:
 - 1.E-mail: Comunicações internas e externas formais que exijam rastreabilidade;
 - 2.WhatsApp Business: Comunicações internas que NÃO exijam rastreabilidade;
 - 3.Zoom: Comunicações internas que NÃO exijam rastreabilidade.
- As ferramentas de comunicação da Objetiva são monitoradas e as mensagens trocadas poderão ser auditadas.

5.3 Internet e rede sem fio

- O uso da internet é monitorado e poderá ser auditado pela equipe de tecnologia da Objetiva e pelo DPO (Encarregado da Proteção de Dados);
- A internet corporativa deve ser utilizada para fins profissionais e de interesse da Objetiva;
- Haverá uma rede pública para ser utilizada de forma livre;
- É proibido o download e armazenamento de softwares e conteúdos protegidos pela lei de propriedade intelectual, como filmes, músicas e livros;
- Não compartilhe a senha do Wi-fi com pessoas externas, ao invés disso, disponibilize a rede de visitantes.



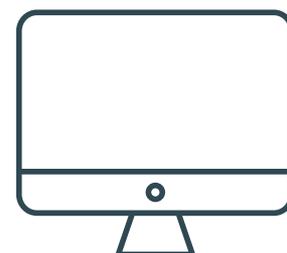
5.4 Impressão e descarte



- Antes de imprimir, pergunte-se se é realmente necessário;
- Após mandar imprimir, dirija-se imediatamente até a impressora selecionada e retire o seu documento;
- Informações classificadas como confidenciais devem ser impressas em impressoras protegidas fisicamente contra o acesso de pessoas não autorizadas;
- Caso seja necessário descartar documentos que contenham dados pessoais ou sigilosos, triture-os de forma que seja impossível identificar os dados que estavam ali contidos;
- A retirada de documentos físicos da Objetiva deve ser consentida pelo gestor direto da área e comunicado ao DPO (Encarregado da Proteção de Dados);
- Documentos que, possuam qualquer tipo de dados pessoais, como nomes, telefones, e-mails e afins, não poderão ser utilizados como rascunho.

5.5 Política da mesa e tela limpa

- Jamais deixe documentos, principalmente aqueles que contenham dados pessoais, visíveis sobre a sua mesa;
- Após a utilização da documentação, guarde-a imediatamente em um local seguro;
- Após a utilização a estação de trabalho, certifique-se de realizar o procedimento de "logoff" (desconectar o usuário conectado no sistema operacional);
- Caso precise se ausentar da frente do seu computador, faça o bloqueio da tela.



5.6 Uso da estação de trabalho

- Todas as estações de trabalho (computadores, dispositivos e afins) são monitoradas pelo setor de tecnologia da informação da Objetiva;
- A estação de trabalho deve ser utilizada exclusivamente para fins profissionais e de interesse da Objetiva;
- O reparo e manutenção das estações de trabalho somente poderão ser realizadas pelo setor de tecnologia da informação;
- Não instale nenhum tipo de software/hardware sem autorização do setor de tecnologia da informação;
- Todos os dados digitais relativos à empresa devem ser mantidos no servidor de arquivos da Objetiva, onde existe um sistema de backup diário e confiável. O setor de tecnologia da informação e o DPO não se responsabilizam por arquivos armazenados na estação de trabalho. Se tiver dúvidas sobre como salvar as informações corretamente, acione o setor de tecnologia imediatamente.



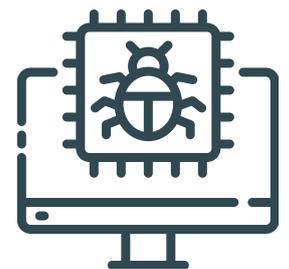
5.7 Política social



- Não comente sobre as rotinas de trabalho da Objetiva para terceiros e/ou em locais públicos;
- Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa;
- Somente aceite ajuda técnica de um membro do setor de tecnologia da informação, previamente apresentado e identificado;
- Não exponha dados sigilosos da Objetiva em redes sociais;

5.8 Malwares e dispositivos removíveis

- Caso perceba mensagens de alerta do seu software de antivírus, como ameaças ou necessidade de atualização, acione o setor de tecnologia da informação imediatamente;
- O uso de dispositivos removíveis, como pendrives e smartphones conectados na estação de trabalho, são proibidos. Exceto os equipamentos corporativos e outras exceções devidamente autorizadas pelo DPO;
- Suspeite de softwares recém-instalados na sua estação de trabalho sem o seu consentimento. Caso isto ocorra, acione imediatamente o setor de tecnologia da informação.



5.9 Dispositivos móveis

- Não registre por áudio ou vídeo quaisquer informações empresariais, exceto quando em caráter publicitário e devidamente acompanhado pela área competente;
- Não grave conteúdos de conversas ou reuniões sem que todos os envolvidos saibam da gravação;
- Não realize a captura de tela (print screen) em informações sigilosas exibidas nas telas de smartphones e tablets.



7. Processo disciplinar

O não cumprimento das diretrizes desta Política de Segurança da Informação poderá acarretar sanções. A análise da gravidade e a aplicação do processo disciplinar será realizada pelo DPO (Encarregado da proteção de dados) com o apoio do comitê de proteção de dados da empresa.

Tais penalidades não excluem a possibilidade de direito de regresso, através de ação judicial em desfavor do funcionário.



Penalidade leve: Advertência verbal e reciclagem obrigatória em segurança da informação.



Penalidade média: Advertência formalizada e suspensão com desconto em folha de pagamento ou multa contratual.



Penalidade grave: Desligamento e/ou rompimento de contrato.

7. Casos omissos e exceções

Os casos omissos e exceções à Política de Segurança da Informação, serão tratados formalmente, através de um processo administrativo interno, liderado pelo Encarregado da Proteção de Dados (DPO) e registrado em ata.



8. Dados de contato importantes

DPO (Encarregado da Proteção de Dados)

dpo@objetivadistribuidora.com.br

Comitê de Proteção de Dados e de Gestão de Incidentes de Segurança

comiteprotecao@objetivadistribuidora.com.br

