

[Celular](#)[Internet](#)[PACOTES](#)[RECARGA](#)[2ª VIA](#)[CONTA ONLINE](#)[APARELHO](#)

SOBRE A OI

[• EMPRESA](#)[• GENTE](#)[• SALA DE IMPRENSA](#)[• REGULAMENTAÇÃO](#)

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

Estabelecer as diretrizes, princípios e responsabilidades além de orientar na execução das ações relacionadas ao tratamento das informações e o uso adequado de ativos pelos colaboradores, estagiários, terceiros, fornecedores, visitantes e partes interessadas nos negócios das empresas do grupo Oi.

2. Definições

As definições dos termos e expressões utilizados neste documento constam no Glossário da Oi.

3. Conteúdo

3.1. Diretrizes

Segurança da Informação: É o conjunto de ações e controles com vista a garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações.

Informação é Patrimônio: Toda informação elaborada, adquirida, manuseada, armazenada, transportada e descartada nas dependências e/ou em ativos das empresas do grupo Oi são consideradas patrimônio da empresa e deve ser utilizada exclusivamente para os interesses corporativos.

Responsabilidade e Comprometimento: Todos os colaboradores, estagiários, terceiros, fornecedores e visitantes, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e salvaguarda dos ativos e informações de que sejam usuários, dos ambientes físicos e computacionais a que tenham acesso, independentemente das medidas de segurança implantadas.

Controle de Acesso: O acesso lógico e o uso da informação da Oi devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao seu cargo ou função.

Gestão de Incidentes de Segurança: Os incidentes de segurança devem ser identificados, monitorados, comunicados e devidamente tratados de forma a impedir a interrupção das atividades e não afetar o

alcance dos objetivos estratégicos da Oi.

Monitoramento: A Oi pode monitorar o acesso e a utilização de seus ativos tecnológicos, como dos ambientes, equipamentos e sistemas da informação, de forma que ações indesejáveis ou não autorizadas sejam detectadas proativamente.

Auditoria e Conformidade: A Oi pode auditar periodicamente as práticas de Segurança da Informação, de forma a avaliar a conformidade das ações de seus colaboradores, estagiários, terceiros, fornecedores e visitantes em relação ao estabelecido nesta Política e na legislação aplicável.

3.2. Princípios de Segurança da Informação

São as bases para as ações ou linhas de conduta de segurança que atuam como guia para a sua implementação e a gestão da Segurança da Informação:

Estabelecer a Segurança da Informação em toda Oi: A Segurança da Informação é tratada em um nível organizacional, de acordo com a tomada de decisões que leve em consideração todos os processos críticos de negócio da Oi.

Adotar uma abordagem baseada em riscos: A Segurança da Informação é fundamentada em decisões baseadas em riscos como perda da vantagem competitiva, conformidade, de responsabilidade civil, interrupções operacionais, danos à reputação e perdas financeiras.

Promover um ambiente positivo de segurança: A Segurança da Informação é estruturada com base no comportamento humano, envolvendo as crescentes necessidades de todas as partes interessadas, visto que o comportamento humano é um dos elementos fundamentais para manter o nível apropriado de Segurança.

3.3. Atribuições e Responsabilidades

3.3.1. Área de Segurança da Informação

- Gerenciar, coordenar, orientar, avaliar e implantar as ações, atividades e projetos relativos à Segurança da Informação na Oi, promovendo ações de interesse da empresa, programas educacionais e de conscientização do capital humano.
- Diminuir o número de incidentes de segurança que causam prejuízos financeiros, problemas com a imagem da Oi e impactos diretos ou indiretos para o negócio da Oi
- Educar, capacitar e conscientizar o capital humano da Oi
- Analisar os desvios e as exceções às orientações desta Política

3.3.2. Colaboradores, estagiários, terceiros, fornecedores, visitantes e partes interessadas das empresas do grupo Oi.

- Conhecer e cumprir as diretrizes estabelecidas nesta Política e demais Regulamentos que compõe a Política de Segurança da Informação da Oi, bem como as boas práticas que contribuem para a Segurança da Informação.
- Reportar ao Gestor imediato e informar a situação identificada através do Canal de Denúncias e Relatos, presente no Canal de Ética na Interativa, as situações que comprometam a segurança das informações nas unidades organizacionais das empresas do grupo Oi.
- Toda informação criada, modificada no exercício de suas funções e qualquer informação contida em mensagens do correio eletrônico corporativo deve ser

tratada como referente ao negócio da Oi, não devendo ser considerada como pessoal, particular ou confidencial, mesmo que arquivadas na sua pasta pessoal. Desta forma, você não deve esperar privacidade pessoal quanto ao uso do correio eletrônico corporativo, pois todas as informações são consideradas propriedade da Oi.

- É proibido compartilhar ou negociar suas credenciais (ID, senha e crachá).

3.4. Compromisso e Penalidades

Todas as garantias necessárias ao cumprimento desta Política estão estabelecidas formalmente com os colaboradores das empresas do grupo Oi. O nosso compromisso é essencial.

O descumprimento da Política é considerado uma falta grave e poderá acarretar na aplicação de sanções previstas em lei, nos regulamentos internos e nas disposições contratuais.

Observe também todas as disposições constantes no Código de Ética disponível na Interativa.

3.5. Treinamento, Atualização e Divulgação

Um programa de conscientização, educação e treinamento em Segurança da Informação necessário à garantia dos objetivos, princípios e diretrizes definidas nesta Política é realizado adequando-se às necessidades e responsabilidades específicas de cada colaborador e estagiário e, onde pertinente, terceiros, fornecedores e visitantes das empresas do grupo Oi.

Da mesma forma, o conteúdo da Política é amplo e constantemente atualizado e divulgado, tanto interna quanto externamente à Oi. Releia-o de tempos em tempos, mesmo que não seja diretamente solicitado.

Sua participação é muito importante.

3.6. Referências

Código de Ética das empresas do grupo Oi.

ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.

ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.

Internet

Planos

Atendimento

ServiçosServiços Adicionais

Pós-Pago

Planos

Atendimento

ServiçosServiços Adicionais

Controle

Planos

Atendimento

ServiçosServiços Adicionais

Pré-Pago

Planos

Atendimento

ServiçosServiços Adicionais



São Paulo, SP ▼

[Empresas](#)

[Investidores](#)

[Sobre a Oi](#)

[Lojas da Oi](#)

[Nossa Marca](#)

[Outras Operadoras](#)