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, parceiros e partes interessadas nos negócios das empresas do grupo Oi.

2 DEFINIÇÕES

Informação: resultante do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe;

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.

Confidencialidade: garantia de que a informação seja acessível ou divulgada somente a pessoas, entidades ou processos autorizados;

Integridade: salvaguarda da exatidão da informação e dos métodos de processamento.

Disponibilidade: garantia de que as pessoas autorizadas obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Conformidade: processo de garantia do cumprimento de um requisito, podendo ser obrigações empresariais com as partes interessadas (investidores, empregados, credores etc) e com aspectos legais e regulatórios relacionados à administração das empresas, dentro de princípios éticos e de conduta estabelecidos pela alta administração da Oi.

Incidente de Segurança da Informação: evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda dos requisitos da Segurança da Informação: confidencialidade, integridade e disponibilidade. Possui uma probabilidade significativa de comprometer os processos de negócios da Oi.

Risco de Segurança da Informação: Risco associados à violação da confidencialidade e integridade, bem como da disponibilidade das informações da companhia nos meios físicos e digitais.

3 CONTEÚDO

3.1 DIRETRIZES

Segurança da Informação: pode ser definida como o conjunto de esforços contínuos para o uso seguro da informação, que contribui para o cumprimento dos objetivos estratégicos da companhia.

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 parceiros, 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, o controle de acesso físico 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.

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 parceiros 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 na análise do comportamento humano, observando as crescentes necessidades de todas** as partes interessadas, através da conscientização e maturidade dos colaboradores fortalecemos 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.

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

- Conhecer e cumprir as diretrizes estabelecidas nesta Política e demais Regulamentos que compõem a Política de Segurança da Informação da Oi;

- Informar as situações que comprometam a segurança das informações nas unidades organizacionais das empresas do grupo Oi, através, do Canal de Denúncias e Relatos, presente no Código de Ética (http://oi.com.br/ArquivosEstaticos/oi/docs/pdf/sobre_oi/codigo-etica-oi.pdf);

- Toda informação criada, modificada no exercício das 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.

- É proibido compartilhar ou negociar suas credencias (ID, senha e crachá);

- Os requisitos de Segurança da Informação devem constar nas aquisições e/ou implementações tecnológicas;

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 ou advertências conforme regulamentos internos e nas disposições contratuais.

Observe também todas as disposições constantes no Código de Ética.

3.5 TREINAMENTO, ATUALIZAÇÃO E DIVULGAÇÃO.

Um programa de conscientização, educação e treinamento em Segurança da Informação é disponibilizado para garantia dos objetivos, princípios e diretrizes definidas nesta Política. O programa deve ser seguido adequando-se às necessidades e responsabilidades específicas de cada colaborador, estagiário, terceiros, fornecedores e parceiros das empresas do grupo Oi.

Da mesma forma, o conteúdo da Política é amplo e constantemente atualizado e divulgado. A releitura desta Política, mesmo que não seja diretamente solicitada, deve ser feita para melhor entendimento. Sua participação é muito importante.

3.6 REFERÊNCIAS

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