1 OBJETIVO

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

2 PÚBLICO ALVO

Colaboradores, estagiários, terceiros, fornecedores, parceiros e outras partes interessadas nos negócios das empresas do grupo.

3 DIRETRIZES

3.1 CONTEÚDO

Informação é Patrimônio: toda informação gerada, adquirida, manuseada, armazenada, sob a guarda, transportada e/ou descartada nas dependências e/ou em ativos das empresas do grupo é considerada patrimônio da organização e deve ser utilizada exclusivamente para os interesses corporativos.

A responsabilidade e o comprometimento deve ser de todos: 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 ou com os quais tenham contato, assim como dos ambientes físicos e computacionais a que tenham acesso, independentemente das medidas de segurança implantadas.

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

Incidentes de Segurança precisam ser tratados: os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados de forma a reduzir riscos no ambiente, evitando interrupção das atividades e não afetar o alcance dos objetivos estratégicos da organização e atendimento dos seus clientes.

Os ativos da organização e sua utilização podem ser monitorados: a organização 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.

A organização pode auditar a conformidade com as práticas de SI: a organização 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, demais regulamentos que a compõem 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 a organização: a Segurança da Informação é tratada em nível organizacional, de acordo com a tomada de decisões que levem em consideração todos os processos críticos de negócio da organização.

Adotar uma abordagem baseada em riscos: a Segurança da Informação é fundamentada em decisões baseadas em riscos como perda da vantagem competitiva, conformidade, responsabilidade civil, interrupções operacionais, danos à reputação e perdas financeiras, uso indevido, fraudes, sabotagens, roubo e ataques cibernéticos.

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, educação e maturidade do capital humano, fortalecendo um dos elementos fundamentais para manter o nível apropriado de Segurança.

3.3 COMPROMISSO E PENALIDADES

Todas as garantias necessárias ao cumprimento desta Política estão estabelecidas formalmente com os colaboradores das empresas do grupo.

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

Todas as disposições legais e demais normas da organização, como o Código de Ética e Conduta, devem ser rigorosamente observadas.

3.4 TREINAMENTO, ATUALIZAÇÃO E DIVULGAÇÃO

A organização conta com um programa contínuo de conscientização de segurança que tem como objetivo conscientizar, treinar e proteger as pessoas, seguindo as melhores práticas internacionais e a política de segurança da empresa, e contribui para disseminação da cultura de Segurança para colaboradores, estagiários, terceiros, fornecedores, parceiros das empresas do grupo e seus clientes.

A organização ainda disponibiliza em seu website material de conscientização, avisos e dicas de segurança para que a comunidade e clientes possam ter acesso facilitado a esse conteúdo.
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 periodicamente para melhor entendimento.

4 PAPEIS E RESPONSABILIDADES

4.1 ATRIBUIÇÕES E RESPONSABILIDADES

A Política de Segurança da Informação é aprovada pelo Conselho de Administração, reforçando o compromisso da alta direção com a melhoria contínua dos processos de segurança e tem designado em sua estrutura corporativa um diretor responsável pela sua gestão.

4.1.1 ÁREA DE SEGURANÇA DA INFORMAÇÃO

- Gerenciar, coordenar, orientar, avaliar e promover a implantação das ações, atividades e projetos relativos à Segurança da Informação na organização, promovendo ações de interesse da empresa, programas educacionais e de conscientização do capital humano.

4.1.2 COLABORADORES, ESTAGIÁRIOS, TERCEIROS, FORNECEDORES, PARCEIROS E PARTES INTERESSADAS DAS EMPRESAS DO GRUPO

- Conhecer e cumprir as normas e orientações estabelecidas nesta Política e demais Regulamentos que compõem a Política de Segurança da Informação da organização;
- Informar as situações que comprometam a segurança das informações através do Canal de Denúncias disponibilizado pela organização para essa finalidade;
- 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 organização, não devendo ser considerada como pessoal, particular ou confidencial, mesmo que arquivadas na sua pasta pessoal;

- Garantir que seja conhecida e cumprida a proibição de compartilhamento ou negociação de credencias (ID, senhas, crachás, tokens e similares);
- Garantir que os requisitos, políticas e processos de Segurança da Informação e de proteção de dados constem nas aquisições e/ou implementações tecnológicas e se mantenham durante seu ciclo de vida.

5 REFERÊNCIAS

Canal de Denuncias: 0800-2822088 (https://www.canalconfidencial.com.br/oi/)
Avisos e dicas de segurança: (https://www.oi.com.br/oi/sobre-a-oi/empresa/informacoes/avisos-e-dicas-de-seguranca)
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.

6 GLOSSÁRIO

- **Autenticidade** - garantia da veracidade da autoria da informação.
- **Confidencialidade** - a informação deve estar disponível e somente ser divulgada a indivíduos, entidades ou processos autorizados;
- **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;
- **Disponibilidade** - as pessoas autorizadas devem obter acesso à informação e aos ativos correspondentes sempre que necessário;
- **Integridade** - salvaguarda da exatidão da informação e dos métodos de processamento;
- **Informação** - é a reunião ou conjunto de dados e conhecimentos resultante do processamento, manipulação e/ou organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe;
- **Incidente de Segurança da Informação** - evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da segurança da informação: confidencialidade, integridade ou disponibilidade.

- **Risco de Segurança da Informação** - riscos associados à violação da autenticidade, confidencialidade e integridade, bem como da disponibilidade das informações nos meios físicos e digitais.
- **Segurança da Informação (SI)** - é o conjunto de ações e controles que tem como objetivo a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos da organização e atendimento dos seus clientes.

7 ANEXOS

Não se aplica

ESTE DOCUMENTO REVOGA VERSÕES ANTERIORES