POLÍTICA

DE

SEGURANÇA DA

INFORMAÇÃO

CONTROLE DE VERSÕES E ALTERAÇÕES					
Versão	**Data**	**Tipo de Alteração**	**Responsável**	**Revisor**	**Aprovador**
01.0	24/11/2023	Criação	Marco Mauricio Tinoco	Comitê de Privacidade	

Sumário

1. OBJETIVO

Expor a todos os clientes, parceiros e colaboradores da **MODAL GESTAO & RESULTADOS LTDA.**, pessoa jurídica de direito privado, inscrita no CNPJ/ME sob o nº 67.201.640/0001-30, com sede na Rua Visconde do Rio Branco, 02, 6º andar, CEP 11013-030, Centro, na cidade de Santos, SP, doravante denominada simplesmente "**MODALGR**" os conceitos relativos à segurança da informação, bem como a importância na adoção das melhores práticas, buscando expor como uma mudança positiva, conscientizando todos os envolvidos nos processos da **MODALGR** ou na interação com terceiros na adoção destas medidas referentes à proteção de dados, considerando as particularidades das atividades desempenhadas pela **MODALGR** nos processos fim-a-fim, que devem ser tratados com toda a atenção e cuidado na garantia da tríade de confidencialidade, integridade e disponibilidade dos dados.

Declarar através desta **Política de Segurança da Informação (PSI)** a determinação da **MODALGR** em adequar-se às leis aplicáveis, fortalecendo o negócio, as parcerias, as relações com clientes e colaboradores, buscando que o resultado não somente traga a adequação à legislação como mero cumprimento de dever legal, mas também que se torne um pilar de confiança dentro das relações da **MODALGR** com seus *stakeholders* internos e externos.

Trazer uma **Política de Segurança da Informação (PSI)** abrangente a **MODALGR**, objetivando atender ao modelo de negócio correspondente às atividades que possam se mostrar diferentes entre si.

1.1. SEGURANÇA DA INFORMAÇÃO

A informação é um dos principais patrimônios do mundo dos negócios e um "ativo" capaz de decidir o sucesso ou o fracasso de toda uma empresa. No entanto, por possuir toda essa importância e somado à crescente facilidade de acesso, a informação se tornou um alvo de constantes ameaças internas e externas.

A **Política de Segurança da Informação (PSI)** é o documento que estabelece as diretrizes e normas, com o intuito de identificar e proteger a informação e os ativos de informação, portanto, deve ser aplicada e cumprida em todas as áreas da empresa.

Esta **Política** ou **PSI** visa garantir:

- A confiabilidade das informações através da preservação da tríade de confidencialidade, integridade e disponibilidade dos dados;
- O compromisso presente em toda a empresa com a proteção das informações de sua propriedade ou sob sua guarda;
- A participação e cumprimento por todos os colaboradores, independente de hierarquia, em todo o processo de segurança;
- A identificação de possíveis violações de Segurança da Informação (SI) e estabelecer ações sistemáticas de controle, monitoramento, prevenção e resposta a incidentes;
- A disponibilidade das informações necessárias a todas as partes interessadas que estejam autorizadas a acessá-las;
- Que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;
- A conscientização, educação e treinamento de todos os colaboradores que utilizam ou detém informações, bem como o uso correto de tais ativos;
- A melhoria contínua da Segurança da Informação (SI).

2. ABRANGÊNCIA

As áreas de Segurança da Informação (SI) e Tecnologia da Informação (TI) são as responsáveis pela salvaguarda dos dados, mas o processo de segurança da informação deve envolver todos os colaboradores, independentemente do nível hierárquico, visto que, de posse de uma informação específica, qualquer pessoa pode por descuido e até mesmo com má intenção, se tornar um agente não autorizado de divulgação de informação.

Diante do exposto, a **Política da Segurança da Informação (PSI)** se aplica a todo o corpo diretivo, consultivo, colaboradores e prestadores de serviços que utilizam os recursos/ativos ou tenham acesso às informações de titularidade da empresa.

3. DEFINIÇÕES

Para efeitos desta **Política da Segurança da Informação (PSI)**, aplicam-se aos conceitos apresentados junto ao **Anexo I** – Siglas e demais conceitos

4. INTRODUÇÃO

Segurança da informação é a proteção da informação aos vários tipos de ameaças a fim de garantir a continuidade dos negócios, minimizar os riscos associados, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*.

Estes controles são estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização, e que também estejam sujeitos a todas as legislações e regulamentações das localidades as quais os serviços ou produtos serão prestados.

A seleção de controles também depende da maneira pela qual esses interagem para prover uma proteção segura. Esta proteção é realizada por meio da preservação da confidencialidade, integridade e disponibilidade das informações, onde:

- A **confidencialidade** é a garantia de que a informação seja acessada exclusivamente por pessoas autorizadas.
- A **integridade** é a garantia de que a informação não seja modificada ou danificada, acidentalmente ou intencionalmente.
- A **disponibilidade** é garantia de que a informação esteja disponível sempre que se necessite dela.

É essencial a criação de políticas, normas, procedimentos e mecanismos de controle para proteger as informações e assim prevenir situações desagradáveis que possam prejudicar os negócios e as pessoas envolvidas, sejam colaboradores ou clientes.

Da mesma forma, as pessoas são fundamentais neste processo. Como colaboradores, devemos proteger as informações que temos acesso em nosso dia a dia e garantir a confiabilidade em nossas relações internas e externas.

5. DIRETRIZES GERAIS

A **Política de Segurança da Informação (PSI)** deve ser divulgada para todos os colaboradores e terceiros.

Todos os colaboradores, parceiros e terceiros devem se comprometer em seguir a **PSI**.

As informações, ativos e sistemas de propriedade da **MODALGR** devem ser utilizados única e exclusivamente para fins profissionais, salvo com prévia autorização de exceção.

Todos os colaboradores, parceiros e terceiros devem proteger e manter a confidencialidade dos dados de clientes de acordo com as normas vigentes na **PSI**.

Todos os acessos físicos às dependências e acessos lógicos aos sistemas da **MODALGR** devem ser autorizados de acordo com a hierarquia de autorização de acessos.

Todos os *softwares* devem estar em conformidade com os termos de licenciamento e com os direitos autorais de propriedade material e intelectual.

Os colaboradores, parceiros e terceiros que infringirem qualquer uma das diretrizes de segurança expostas neste instrumento estarão passíveis de penalidades ou sanções.

6. PRINCÍPIOS FUNDAMENTAIS DE SEGURANÇA DA INFORMAÇÃO

Nesta **PSI** são listados alguns princípios fundamentais de segurança da informação, porém, tais princípios não estão limitados nesta política e podem estar detalhados em outras políticas da organização.

Toda informação produzida ou por ela adquirida é propriedade da **MODALGR** e faz parte de seu patrimônio, não importando a forma de apresentação ou armazenamento.

Os recursos e as informações são disponibilizados aos colaboradores, parceiros e terceiros exclusivamente para o exercício de suas atividades em prol da **MODALGR**, e o uso dos recursos tecnológicos e das informações deve sempre respeitar o disposto nas normas e procedimentos internos.

A prevenção contra incidentes é uma responsabilidade de todos, por isso devemos estar informados sobre quais as medidas que precisamos tomar prontamente na ocorrência deles. Os colaboradores, parceiros e terceiros devem estar sempre atentos aos procedimentos que garantam a continuidade dos nossos processos e atividades críticas.

Os ativos de informação devem ser classificados de acordo com sua importância e protegidos contra falhas, mau uso, divulgação ou modificações não autorizadas e demais eventuais incidentes de segurança da informação.

Os recursos que compõem a infraestrutura de tecnologia e segurança devem ser devidamente usados e gerenciados pelas áreas responsáveis, para suportarem de forma adequada as demandas e nossos processos de negócio.

A disseminação da cultura sobre segurança da informação é um compromisso permanente de todos e exige a prática diária.

A **MODALGR** busca inovações e está atenta às novas tecnologias, visando sua aplicação de forma preventiva, antecipando as possíveis oportunidades e evitando as vulnerabilidades e os impactos nos processos de negócio.

Os riscos de comprometimento da **confidencialidade, integridade e disponibilidade** dos ativos de informação devem ser permanentemente identificados, avaliados e tratados de acordo com sua criticidade.

As relações com os parceiros de negócio devem pautar-se pelo respeito mútuo, pela ética e transparência nas negociações e pelo respeito aos contratos celebrados. No caso de contrato de prestação de serviço, deve ser estabelecido acordo de confidencialidade entre as empresas e demais requisitos de segurança necessários.

Os requisitos legais, regulamentares e estatutários pertinentes à área de atuação da organização e os direitos de propriedade intelectual devem ser observados e seguidos por todos os colaboradores, parceiros, terceiros prestadores de serviço.

Todos os colaboradores, parceiros e terceiros são responsáveis por proteger as informações e relatar qualquer situação que represente desvio ou violação de segurança.

Qualquer violação à política, às normas e aos procedimentos de segurança da informação, observadas sua natureza e gravidade, estão sujeitas à aplicação do competente procedimento disciplinar da **MODALGR**, nos termos da legislação ou, conforme o caso, das penalidades previstas nos contratos de prestação de serviços.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação é uma atividade essencial para a gestão de segurança da informação dentro de uma organização e deve ser viabilizada através de um procedimento que deverá ser utilizado pelos colaboradores, parceiros e terceiros que estiverem desempenhando atividades dentro da **MODALGR** ao manipular, editar ou criar documentos que possuem informações de propriedade da **MODALGR**.

O usuário deverá classificar as informações seguindo os seguintes níveis:

- **Confidencial**
- **Restrita**
- **Interna**
- **Pública**

A segurança da informação possui o direito de monitorar todo e qualquer conteúdo que estiver sendo enviado para fora da **MODALGR**, com a possibilidade de bloquear preventivamente o envio de informações que são de cunho confidencial, restrita e interna apenas à **MODALGR** ou que em ocasiões específicas podem ter sido classificadas de maneira incorreta.

Destaca-se que a classificação dos tipos e classes de informação é uma atividade interna da **MODALGR**, a qual é criada e gerida através de diretivas originarias na alta administração.

Com aplicação deste procedimento por parte dos colaboradores, parceiros e terceiros, espera-se que a **MODALGR** consiga garantir os seguintes itens:

- Reduzir o risco de informações classificadas como confidencias, restritas e internas sejam acessadas por pessoas não autorizadas;
- Reduzir o risco de perda de integridade das informações confidenciais, restritas e internas, criando maior valor para o negócio;
- Educar os colaboradores, parceiros, terceiros prestadores de serviço;
- Entre outros ganhos imensuráveis.

As informações coletadas, processadas e armazenadas na infraestrutura de tecnologia da informação devem ser acessíveis apenas as pessoas, a processos ou a entidades autorizadas, a fim de garantir a confidencialidade das informações.

8. SIGILO E CONFIDENCIALIDADE DAS INFORMAÇÕES

A confidencialidade e o sigilo são essenciais no tipo de serviço que prestamos, sendo fundamentais para a relação de confiança e respeito com nossos clientes. Uma informação confidencial, restrita ou interna divulgada para pessoas indevidas prejudica a **MODALGR**, colocando em risco a reputação e confiabilidade que possuímos perante os diferentes públicos com os quais nos relacionamos, sejam colaboradores, parceiros, terceiros, clientes, acionistas entre outros, ocasionando, muitas vezes, perdas financeiras.

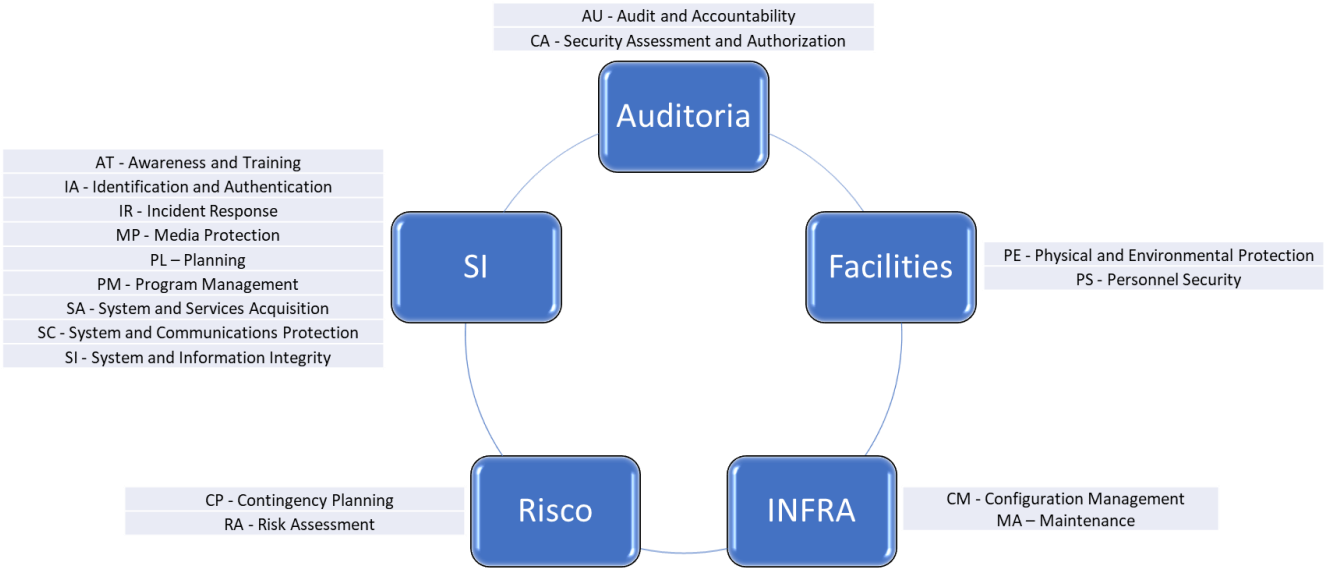
É imprescindível a conscientização de todos os colaboradores, parceiros e terceiros em relação ao sigilo e confidencialidade das informações que lidamos em nossas atividades, além da obrigação em atender às legislações, normas e regulamentos aplicáveis ao nosso negócio. Toda a organização que deseja manter-se viva, alcançar seus objetivos e missão, deve preservar a confidencialidade de suas informações. Por isso, nossa informação deve ser acessada e utilizada somente por quem precisa dela para a realização de suas atividades.

Portanto, os colaboradores, parceiros e terceiros devem ter ciência e garantir que todas as informações as quais tiverem acesso no exercício de suas atividades serão divulgadas ou compartilhadas com pessoas ou entidades não autorizadas. Caso isso seja necessário ao exercício de suas atividades, os colaboradores, parceiros e terceiros sempre adotarão as melhores práticas de segurança da informação durante todo o ciclo de vida dos dados dentro ou fora da **MODALGR**.

Em nosso Portal junto a área de *Compliance* (https://www.modalgr.com.br/compliance/), é possível acessar aos respectivos Códigos de Conduta e Ética, bem como nas áreas de Privacidade e Segurança da Informação há uns capítulos destinados à segurança da informação e propriedade intelectual, que complementa essas observações, bem como este documento.

9. PAPÉIS E RESPONSABILIDADES DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Com base nas diretrizes expostas e em concordância com a Estratégia Nacional de Segurança Cibernética, que recomenda o uso de controles do NIST, foram definidos os papéis e responsabilidades das áreas da **MODALGR**. O *National Institute of Standards and Technology* (NIST) é reconhecido mundialmente como um código de prática de segurança da informação - https://nvd.nist.gov/800-53/Rev4.



A responsabilidade pela proteção dos ativos de informação da **MODALGR** não deve ser apenas da estrutura da Auditoria, *Facilities*, Infra, Risco e Segurança da Informação, e sim de todo o corpo diretivo, colaboradores, parceiros, terceiros e prestadores de serviço da **MODALGR** através do cumprimento das políticas definidas e da assunção de obrigações em contratos específicos firmados.

9.1. PAPÉIS E RESPONSABILIDADES DAS PESSOAS

9.1.1. Alta Direção

Alta Direção é uma pessoa ou um grupo de pessoas que dirige e controla a **MODALGR** no nível mais alto. A Alta Direção tem o poder de delegar autoridade e prover recursos na organização. Constitui-se de cargos de diretores ou superiores dentro da **MODALGR**. É responsável por:

Estar alinhada e comprometida com a política de segurança da informação, bem como suas normas e procedimentos.

- Definir responsabilidades e alocar os recursos necessários para a implantação e manutenção dos diversos controles de segurança da informação.
- Definir uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.
- Realizar análises críticas dos sistemas de gestão de segurança da informação.
- Promover o desenvolvimento da cultura em segurança da informação conforme estabelecido nas políticas e procedimentos da organização, demonstrando seu apoio às políticas, procedimentos e controles, agindo como tal, de forma exemplar.

- Assegurar que as metas de segurança da informação estejam identificadas, atendam aos requisitos da organização e estejam integradas nos processos relevantes.
- Formular, analisar criticamente e aprovar a política de segurança da informação.
- Analisar criticamente a eficácia da implementação da política de segurança da informação.
- Prover um claro direcionamento e apoio para as iniciativas de segurança da informação.
- Fornecer os recursos necessários para o sistema de gestão de segurança da informação.
- Aprovar as atribuições de tarefas e responsabilidades especificas para a segurança da informação.
- Apoiar programas para manter a conscientização da segurança da informação.
- Assegurar que a implementação dos controles de segurança da informação tem uma coordenação e permeia a organização.
- Identificar as necessidades para a consultoria de um especialista interno ou externo em segurança da informação, analise criticamente e coordene os resultados desta consultoria por toda a organização.

9.1.2. Pessoas & Cultura

Fazem parte da área de Gestão e Pessoas qualquer colaborador responsável pela administração dos recursos humanos disponíveis na empresa. É responsável por:

- Difundir os principais pontos das Políticas de Segurança durante a integração de novos colaboradores, parceiros e terceiros.

- Apresentar e garantir a assinatura dos termos aplicáveis, no número de cópias necessário e endereçar a salvaguarda dos documentos às áreas internas responsáveis.
- Avaliar em conjunto com a gestão de segurança da informação ações periódicas de conscientização e reciclagem do tema aos colaboradores, parceiros e terceiros.
- Comunicar e solicitar imediatamente às áreas responsáveis o recolhimento de chaves e crachás e revogação de outras concessões que garantam o acesso às instalações físicas.
- Solicitar a revogação do acesso aos sistemas de informação corporativos, conexões remotas, e-mails e quaisquer outros meios de acesso à informação e/ou comunicação corporativa ao departamento de tecnologia da informação.
- Garantir que ativos da empresa sejam devolvidos.
- Divulgar a relevância do tema segurança da informação durante a contratação de um colaborador, parceiro ou terceiro .

9.1.3. Líderes

Líderes são os colaboradores responsáveis hierarquicamente por um ou mais colaboradores, parceiros e terceiros. Constitui e não é limitado a cargos de coordenadores, gerentes e superintendentes. É responsável por:

- Garantir que as normas de segurança da informação sejam seguidas em seu departamento.
- Promover o desenvolvimento da cultura em segurança da informação por meio do exemplo, disseminando e verificando o cumprimento dos controles, bem como orientando os colaboradores, parceiros e terceiros prestadores de serviço sob sua gestão.

- Confirmar que os acordos de sigilo e responsabilidade foram conhecidos e assinados por todos.
- Informar imediatamente a direção de gestão e pessoas quando um colaborador, parceiro ou terceiro for desligado da empresa ou transferido para outra localidade.
- Saber que é responsável tanto pelo acesso lógico de todos os colaboradores, parceiros e terceiros da sua equipe aos sistemas da **MODALGR**, quanto as ações executadas por eles.
- Zelar pela proteção das informações e dos recursos relacionados à sua área, fornecendo parâmetros de classificação condizentes com a criticidade dos mesmos e controlando os privilégios de acesso dos colaboradores, parceiros e terceiros sob sua gestão de acordo com as atividades que desempenham.
- Realizar a gestão dos riscos relativos aos processos de negócio e ativos sob sua responsabilidade.
- Criar e publicar os procedimentos complementares necessários para o controle dos requisitos de segurança da informação específicos de suas unidades de negócio.

9.1.4. Líder da Informação

Líder da informação é todo colaborador responsável por um ou mais ativos de informação. Esses ativos podem ser bancos de dados e arquivos de dados, documentação de sistemas, manuais de usuário, material de treinamento, procedimentos operacionais ou de suporte, planos de continuidade, informações em arquivos, propostas comerciais, laudos etc. É responsável por:

- Definir a classificação da informação sob sua responsabilidade e revê-la periodicamente.

- Garantir a proteção das informações sob sua responsabilidade, conforme a classificação definida pela política de segurança da informação.
- Definir junto à gerência de segurança da informação quais usuários ou grupos de usuários tem real necessidade de acesso à informação, identificando e avaliando os perfis de acesso, conforme a necessidade do negócio.
- Interagir com as áreas responsáveis sempre que identificada a necessidade de redefinição de perfis de acesso.
- Autorizar ou revogar os acessos às informações e sistemas.
- Revalidar periodicamente (no mínimo, uma vez por ano), as autorizações dos usuários que utilizam os ativos de informação.
- Solicitar o cancelamento do acesso/autorização dos usuários que não tenham mais necessidade de acesso à informação.
- Agir em conjunto com a diretoria de gestão e pessoas na formalização imediata de desligamentos de colaboradores, parceiros ou terceiros, com a finalidade de serem revogados seus acessos a sistemas e informações corporativas.
- Analisar os relatórios de auditoria e os desvios de controles de segurança ou comportamental relacionados aos ativos de informação.
- Participar da investigação dos incidentes de segurança da informação, fornecendo todas as informações e autorizações solicitadas.
- Conhecer a respectiva criticidade das informações aos negócios da **MODALGR**, o fluxo desta nos processos internos e os agentes que interagem com ela, a fim de que o ativo de informação seja adequadamente classificado, de forma que permita que os controles preventivos sejam dimensionados e aplicados adequadamente.

- Delegar a sua “autoridade de segurança” para outro colaborador, isto é, o poder de agir em relação à segurança, porém, mantendo a responsabilidade final pela proteção do ativo de informação.

9.1.5. Colaboradores, Terceiros e Prestadores de Serviços

Colaboradores são todos aqueles que fazem parte do quadro de recursos humanos. Prestadores de serviço são todos aqueles que prestam serviços internos ou externos. São responsáveis por:

- Conhecer a política de segurança da informação da **MODALGR** bem como os demais controles e procedimentos relacionados à mesma e aplicáveis às atividades desempenhadas.
- Apoiar a divulgação das diretrizes da **PSI** no respectivo departamento.
- Ler e assinar o termo acordo de confidencialidade.
- Utilizar os recursos tecnológicos e as informações em caráter estritamente profissional, limitado ao âmbito de suas atividades e observando sempre os requisitos de ética.
- Ser responsável ao utilizar os recursos de TI da empresa: computadores, e-mails, mídias, Intranet e Internet etc.
- Manter o sigilo das informações que você tem acesso ou conhecimento.
- Garantir que as informações que você divulga aos clientes são verdadeiras.
- Seguir todas as regras de segurança da informação.
- Consultar a política de segurança da informação e as normas relacionadas, o líder da área ou a equipe de segurança da informação sempre que tiver dúvidas de como agir.

- Proteger as informações às quais tenha acesso, garantindo que recebam o tratamento adequado de acordo com sua classificação e procedimentos em respeito ao compromisso de sigilo profissional assumido.
- Fazer uso seguro de dispositivos de autenticação corporativos, tais como o crachá, as chaves e suas correspondentes senhas e os certificados digitais, que devem ser usados de forma individual e não podem ser compartilhados em hipótese alguma.
- Relatar imediatamente quaisquer situações de violação ou que possibilitem a violação dos controles de segurança da informação que venha a tomar conhecimento.
- Observar estritamente as disposições contidas na política de segurança de informação e suas atualizações, as quais se encontram disponíveis no sistema de gestão da qualidade.
- Atentar-se à classificação das informações que manipula e evitar que ela seja distribuída de forma inadequada ou torne-se disponível a pessoas cujo acesso não foi autorizado.
- Zelar pelos equipamentos de tecnologia e ativos de informação a que tiver acesso, a fim garantir a segurança da informação.
- Reportar qualquer suspeita de violação de segurança e comportamentos em não conformidade com as diretrizes contidas na política de segurança da informação e, bem como todos os incidentes de segurança ocorridos, à gerência de segurança da informação.
- Colaborar com os programas de conscientização promovidos pela diretoria de gestão e pessoas e gerência de segurança da informação.
- Ter ciência das políticas definidas de modo a adotar medidas preventivas ao tratamento adequado das informações, e contatar as áreas responsáveis em situações de dúvida.

- Observar e respeitar que os direitos de propriedade intelectual, sabendo que estes direitos recaem tanto sobre ativos tangíveis quanto intangíveis, incluindo as marcas, as patentes, os códigos-fonte, os contratos de licenciamento entre outros.
- Garantir que todos os ativos da empresa em posse daquele colaborador (notebooks, mídias, computadores de mão, celulares, rádios etc) devem ser protegidos quando estiverem em áreas públicas e acessados somente para assuntos referentes ao trabalho. Em caso de perda ou furto, deve ser notificação imediatamente o gestor direto e a Gerência de TI.
- Ter ciência que qualquer informação que é acessada, transmitida, recebida ou produzida na **MODALGR** está sujeita a divulgação e auditoria pelas partes relevantes. Colaborador pode sofrer medidas legais e/ou profissionais caso acesse, transmita ou gere informações de conteúdo ilegal, malicioso, impróprio ou que conflite ou contrarie os valores e interesses da **MODALGR**.

9.1.6. Segurança da Informação

A Segurança da Informação está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade. É responsável por:

- Monitorar os recursos e os ambientes sob a sua responsabilidade com o objetivo de garantir a proteção contra as possíveis ameaças e o uso inadequado, assim como mantê-los em dia com as suas atualizações e com as mudanças na legislação e/ou nos requisitos do negócio.
- Gerenciar os controles e as ferramentas de segurança da informação, assim como tratar os incidentes, problemas, mudanças e quaisquer requisições e/ou reportes relacionados à segurança da informação.

- Analisar de forma sistemática e periódica os controles, incluindo a política, as normas e os procedimentos de segurança da informação, para que eles se mantenham efetivos, pertinentes e aderentes aos requisitos do negócio.
- Operacionalizar e fornecer apoio às atividades de segurança da informação no ambiente de TI e nos demais processos nas diversas áreas de negócio.
- Desenvolver e manter a políticas de segurança da informação.
- Desenvolver e conduzir um plano anual de iniciativas de segurança da informação.
- Interagir com as áreas de Infraestrutura de TI e sistemas na avaliação de impactos e riscos no desenvolvimento, homologação e na gestão de mudanças do ambiente de tecnologia.
- Desenvolver, em conjunto com a diretoria de gestão e pessoas, ações de disseminação da cultura de segurança da informação.
- Elaborar e propor iniciativas voltadas à manutenção e evolução do nível de segurança, a serem validadas e patrocinadas pelo comitê de gestão de riscos.
- Avaliar os riscos associados à segurança da informação, identificando previamente potenciais riscos à confidencialidade, integridade e disponibilidade.
- Coordenar a implantação das medidas preventivas e corretivas.
- Fiscalizar, analisar, reportar e coordenar a resposta de incidentes de segurança da informação.
- Elaborar relatórios periódicos contendo indicadores de segurança e progressos.
- Administrar o acesso lógico aos sistemas, respeitando as políticas aplicáveis.
- Fornecer credenciais iniciais de acesso aos usuários conforme solicitação devidamente aprovada e registrada pela área de gestão e pessoas.
- Fornecer, após as devidas autorizações, acesso aos usuários de acordo com o papel deste na **MODALGR**.

- Garantir que os usuários tenham acesso somente às informações a que foram autorizados pelo respectivo líder.
- Garantir o armazenamento e retenção de logs quanto ao acesso a serviços de rede, aplicações, sistemas e ativos de informação que estejam integrados ao SIEM, para que exista visibilidade e análise de incidentes de segurança.
- Analisar preventivamente arquivos de registros de auditoria (logs) e similares, bem como as mensagens enviadas pelo sistema operacional no intuito de identificar desvios de segurança e outros eventos que possam comprometer a disponibilidade e bom funcionamento deles.
- Analisar tecnicamente as soluções que a **MODALGR** deseja utilizar, comprar ou homologar, seguindo os critérios definidos pela área de segurança da informação.

Mediante essas diretrizes e em concordância com a Estratégia Nacional de Segurança Cibernética, que também recomenda o uso de controles do CIS (https://www.cisecurity.org/controls/cis-controls-list), abaixo estão outras diretrizes de segurança da informação:

- Governança de Segurança Cibernética:
- realizar fóruns de governança de segurança da informação.
- criar controles para o tratamento de informações com restrição de acesso.
- estabelecer requisitos mínimos de segurança cibernética nas contratações da **MODALGR**.
- implantar programas e projetos sobre governança cibernética.
- adotar, além das diretrizes da **PSI**, padrões e modelos de governança reconhecidos mundialmente (NIST, CIS etc.).
- adotar, padrões de segurança no desenvolvimento e aquisição de novos produtos desde sua concepção (*Privacy/Security by Design and Default*).

- recomendar a adoção de soluções de criptografia, observada, para tanto, a legislação específica.
- intensificar o combate à pirataria de software.
- recomendar a certificação em segurança cibernética e ampliar o uso do certificado digital.
- realizar exercícios cibernéticos com participação de múltiplos atores.

9.2. SOAR - Security Orchestration Automation and Response (a ser instituido, hoje sob gestão da Segurança da Informação):

- sistemas de proteção de *endpoints* e servidores.
- segurança de e-mail.
- segurança de roteadores, switches, dispositivos Wireless e demais pontos de acesso à rede.
- utilização de firewalls.
- proteção dos sistemas de arquivos.
- uso de IDS (Intrusion Detection System) ou IPS (Intrusion Prevention System).
- utilização de SIEM.

9.3. Estratégia de Implementação em Segurança da Informação

Com base em todo o cenário, nas diretrizes e aderência a Estratégia de Segurança, deve ser adotado o modelo CIS (Center for Internet Security), que prevê controles do tipo *Basic, Foundational* e *Organizational*:

CIS Top 20 Critical Security Controls

- O CIS Top 20 é um conjunto controles projetados para ajudar as organizações a proteger seus sistemas e dados contra vetores de ataque conhecidos.
- Controles são mapeados para vários standards de conformidade (NIST Cybersecurity) e regulamentos (PCI DSS e HIPAA).
- Os controles são baseados nas informações mais recentes sobre ataques comuns e refletem o conhecimento combinado de especialistas forenses, pentesters e colaboradores de agências governamentais dos EUA.

Observações
- Basic CIS Controls – INFRA: 1. Inventory and Control of Hardware, 2. Inventory and Control of Software
- Foundational CIS Controls – INFRA: 10. Data Recovery Capabilities

9.4. Violações e Penalidades

Violações a esta **PSI** também serão consideradas como violação ao Código de Ética e Conduta da **MODALGR**, sujeitando seus infratores às penalidades disciplinares cabíveis, incluindo advertências, suspensões, além de demissões por justa causa, dentre outras. Os Administradores e Colaboradores responderão legalmente, além de disciplinarmente, quando aplicável. Os Terceiros responderão civilmente e criminalmente por infrações a esta política, com aplicação das penalidades contratuais previstas, além de eventuais perdas e danos cabíveis.

Aquele que detectar violações a esta **PSI**, deverá comunicar o fato ao Comitê de Ética e Conduta da **MODALGR**, o que poderá ser realizado mediante envio de denúncia ao Canal de Conduta, mantendo o nome do denunciante em anonimato ou não, a seu exclusivo critério.

Ao Comitê de Conduta caberá analisar e deliberar acerca da aplicação de penalidades administrativas ao infrator e/ou demais medidas judiciais aplicáveis. A área de Segurança da Informação apoiará na apuração das causas e os efeitos do incidente ocorrido, para então tomar as medidas de mitigação e contenção.

O não cumprimento desta **PSI** pode gerar riscos de segurança da informação, financeiros, vazamento de informações, uso impróprio da informação, afetar negativamente a imagem da organização bem como não garantir a confidencialidade, integridade e disponibilidade da informação.

9.5. Termo de Sigilo e Responsabilidade (NDA)

Este termo é utilizado para que todo e qualquer colaborador, parceiro/terceiro se comprometa formalmente a seguir a política de segurança da informação vigente. Sendo assim, a ciência das sanções e punições ao seu não cumprimento é de conhecimento de todos.

A responsabilidade pela guarda e revisão periódica dos termos de sigilo e responsabilidade assinados é da área de Gestão e Pessoas.

9.6. Exceções e Esclarecimentos

Mediante o surgimento de fatos relevantes que não tenham sido contemplados neste documento, bem como a análise da possibilidade de exceção a algum item descrito nesta **PSI** (Política de Segurança da Informação), por ser passível de risco(s), todo e qualquer pedido de exceção ou dúvida deverá ser encaminhado à área de riscos, que por sua vez fará a avaliação e a tomada de decisão conjunta.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da **MODALGR**, ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela **MODALGR**.

10. REFERÊNCIAS

ABNT(2013). NBR ISO IEC 27001 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos

ABNT(2013). NBR ISO IEC 27002 – Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação

The 20 CIS Controls & Resources

https://www.cisecurity.org/controls/cis-controls-list

National Institute of Standards and Technology – Security and Privacy Controls for Federal Information Systems and Organizations

https://nvd.nist.gov/800-53/Rev4

Estratégia Nacional de Segurança Cibernética

http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm

11. CONSIDERAÇÕES FINAIS

O presente documento deve ser lido e interpretado sob a égide das leis competentes, em português, em conjunto com as Normas e Procedimentos aplicáveis pela MODALGR.

Havendo incorporação ou fusão de MODALGR e, portanto, transferência ou compartilhamento de bases com dados pessoais, o DPO (Encarregado de Proteção de Dados Pessoais) deverá notificar os Titulares destes dados a respeito da mudança organizacional, bem como facultar-lhe a oposição ao tratamento de seus dados, desde que o tratamento seja baseado no Consentimento.

Esta Política, bem como as demais Normas e Procedimentos da MODALGR, encontram-se no website. Em caso de indisponibilidade, podem ser solicitadas ao DPO (Encarregado de Proteção de Dados Pessoais).

12. INFORMAÇÕES DE CONTROLE

Esta política terá vigência a partir do dia de sua publicação.

A atualização desta norma ocorrerá anualmente, ou quando ocorrerem alterações significativas no ambiente de negócios da **MODALGR** que justifiquem sua atualização.

Anexo I – Siglas e demais conceitos

SIGLA	DESCRIÇÃO
AMEAÇA	Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
ANONIMIZAÇÃO	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento para retirar a possibilidade de associação, direta ou indireta, do dado a um indivíduo.
ANPD	Autoridade Nacional de Proteção de Dados - ANPD, é a Autoridade Competente na condição de Órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais.
ATIVO	Qualquer coisa que tenha valor e que precise ser adequadamente protegido.
ATIVO INTANGÍVEL	Todo elemento que possui valor e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando a dados, reputação, imagem, marca ou conhecimento.
ATIVOS DE INFORMAÇÃO	São bancos de dados e arquivos de dados, documentação de sistemas, manuais de usuário, material de treinamento, procedimentos operacionais ou de suporte, planos de continuidade, informações em arquivos.
BANCO DE DADOS	Conjunto estruturado de dados, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
COLABORADOR	Empregado, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venham a ter relacionamento profissional, direta ou indiretamente.
COMPANHIA	São todas as empresas que compõem a **MODALGR** e outras controladas, coligadas e subsidiárias.
COMPARTILHAMENTO DE DADOS	Comunicação, difusão, transferência nacional ou internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos, entidades ou pessoas, e para uma ou mais modalidades de tratamento.

CONFIDENCIALIDADE	Propriedade da informação onde a mesma não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
CONSENTIMENTO	Manifestação livre, informada e inequívoca pela qual o Titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
CONTA DE ACESSO / LOGIN	Símbolo ou sequência de caracteres usados por um sistema para identificar um usuário específico de forma a garantir sua unicidade.
CONTROLADOR	Pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
DADO ANONIMIZADO	Dado que não identifica de forma direta ou indireta um Titular, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
DADO PESSOAL	Informação relacionada à pessoa física identificada ou identificável. Para os propósitos desta Política, os dados pessoais são classificados como Informação Confidencial, abrangendo dados pessoais de cliente, parceiros, fornecedores e colaboradores.
DADO PESSOAL SENSÍVEL	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa física.
DISPONIBILIDADE	Propriedade da informação ser acessível e utilizável sob demanda por uma entidade autorizada.
DPO	Encarregado de Proteção de Dados (DPO – Data Protection Officer) deve ser uma pessoa, natural ou jurídica, indicada pelo controlador, para atuar principalmente, como um canal de comunicação entre o agente de tratamento, os titulares dos dados e a ANPD.
EVENTO	Algum acontecimento que mude o estado atual de um processo.
HARDWARE	Unidades físicas, componentes, circuitos integrados, discos e mecanismos que compõem um computador ou os seus periféricos.
INCIDENTE DE SEGURANÇA	Qualquer evento que resulte em perdas ou danos aos ativos da **MODALGR**, ou qualquer ação que desrespeite as regras de segurança. Considera-se também incidente de segurança toda e qualquer forma de tratamento inadequado, ilícito ou indevido de dados.

INCIDENTE DE SEGURANÇA DA INFORMAÇÃO	Um ou mais eventos indesejados ou inesperados que possam comprometer a segurança das informações e enfraquecer ou prejudicar as operações comerciais, podendo também resultar em violação da segurança.
INFORMAÇÃO CONFIDENCIAL	Informação que é de grande importância para a organização, sua divulgação indevida pode causar algum dano ou prejuízo à Companhia. Toda informação ou ativos de informação aos quais o colaborador tiver acesso em razão do exercício de duas atividades para a Companhia, seja essa informação classificada como Confidencial, Restrita ou Interna.
INTEGRIDADE	Propriedade da exatidão e integridade da informação.
MALWARES	O nome malware vem do inglês malicious software (programa malicioso). Refere-se a qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao computador.
OPERADOR OU PROCESSADOR	Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.
PHISHING	Mensagens de e-mail que solicitam dados do usuário de forma direta ou através de redirecionamentos para sites ou números de telefone, a fim de roubar sua identidade.
PSEUDOANONIMIZAÇÃO	É o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
PSI	Política de Segurança da Informação (**PSI**) é o documento que estabelece as diretrizes e normas, com o intuito de identificar e proteger a informação e os ativos de informação.
RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS	Documento que contém a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos Titulares de dados, bem como medidas, salvaguardas e mecanismos de mitigação desses riscos.
RISCO	Combinação da probabilidade de ocorrência de um evento e seus respectivos impactos.
SOAR	SOAR é o termo utilizado para denominar o processo de automação de respostas a incidentes da companhia.

SOFTWARE	Qualquer programa ou grupo de programas que instrui ao hardware sobre a maneira como ele deve executar uma tarefa, inclusive sistemas operacionais, processadores de texto e programas de aplicação.
SOLICITAÇÃO DE TITULAR DE DADOS	Requisição do Titular de dados acerca de seus direitos estabelecidos em lei e relativos ao processamento dos seus dados pessoais.
SPAM	Termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.
TITULAR	Pessoa física a quem se referem os dados pessoais que são objeto de tratamento.
TRATAMENTO DA INFORMAÇÃO	Uso adequado da informação de acordo com as diretrizes estabelecidas nos diversos cenários que ocorrem no dia a dia (armazenamento, transmissão, descarte, impressão etc).
VIOLAÇÃO DE DADOS	Destruição, perda, alteração, divulgação acidental ou ilegal, não autorizada ou acesso a dados pessoais transmitidos, armazenados ou de outra forma processados, resultante de incidente de segurança.
VULNERABILIDADE	Fragilidade de um ativo que pode ser explorada e gerar danos à organização.