Política de Segurança da Informação e Cibersegurança

Janeiro de 2021

Introdução

A Política de Segurança da Informação diz respeito a iniciativas para a proteção da informação gerada e armazenada dentro da **Mirante Investimentos LTDA**, auxiliando a empresa a cumprir com sua atividade de forma ética e correta. Quando não são gerenciadas de modo correto, estas informações podem causar dano à **Mirante Investimentos LTDA**, prejudicar a imagem da empresa, o crescimento e desenvolvimento do negócio.

A informação pode estar presente na **Mirante Investimentos LTDA** de diferentes maneiras, tais como: banco de dados e diretórios de rede, documentos impressos, documentos eletrônicos, equipamentos portáteis, comunicação oral ou comunicação por telefone. Portanto, a empresa entende que toda informação gerada e desenvolvida nas dependências de seu site, durante a execução das atividades, constitui um ativo e deve ser utilizada única e exclusivamente para a finalidade a qual foi autorizada.

A Política de Confidencialidade, Segurança da Informação e Cibersegurança ("Política") tem como objetivo estabelecer princípios e diretrizes de proteção destas informações. Esta política se aplica a todos os colaboradores da Mirante Investimentos Ltda.

Proteção

A **Mirante Investimentos LTDA** possui como diretriz proteger a informação, independente da forma apresentada, de riscos e ameaças que possam comprometer a confidencialidade, integridade e disponibilidade destas.

- **Confidencialidade:** garantir que as informações sejam de conhecimento e divulgação exclusiva a pessoas autorizadas.
- **Integridade:** garantir que as informações armazenadas sejam íntegras, sem modificações e erros indevidos, sejam estes propositais ou acidentais.
- **Disponibilidade:** garantir que as informações estejam disponíveis a pessoas autorizadas para o correto exercício de suas atividades.

Desta forma, a empresa busca zelar pelos seus sistemas internos, de modo a garantir que as informações por eles geradas, armazenadas, processadas e disponibilizadas sejam confiáveis e seguras. Para isso, de maneira geral são adotados alguns procedimentos, tais como:

- Cada Colaborador possui um login individual para acesso as máquinas, base de dados, sessões, arquivos e programas específicos sendo que este login restringe o acesso do Colaborador somente às informações que lhe são competentes as atividades diárias, além de permitir rastrear alterações em dados, arquivos e programas promovidos por este usuário;

- Todas as planilhas eletrônicas são bloqueadas por senhas (comuns e individuais dependendo do caso) a fim de evitar perda de informações ou dados por motivos e erros operacionais;

- Há 2 backups diários de todas as informações e dados da empresa sendo que um é realizado em servidor na Nuvem (Microsoft Azure) e outro fisicamente através de HD Externo localizado em área de acesso restrito;

- O sistema de nobreaks assegura certa autonomia para que atividades não sejam interrompidas de forma abrupta num eventual cenário de falta de energia;

- Há um sistema de gravação telefônica que captura todos os ramais;

- Acesso as instalações da **Mirante Investimentos LTDA** são realizados por controle de acesso na portaria do edifício, o acesso é restrito aos Colaboradores autorizados, demais acessos de pessoas são controlados pela portaria e previamente anunciados e autorizados.

Além disso, a **Mirante Investimentos LTDA** considera que todos os dados e comunicações transmitidas através, recebida por ou contidas nos equipamentos eletrônicos de comunicação da empresa são de propriedade desta. Dessa forma, estão sujeitos às regulamentações e políticas internas aplicáveis e, portanto, a empresa se reserva o direito de monitorar, rever e torná-los públicos se assim o julgar necessário.

Definições

Informações Confidenciais

São consideradas informações confidenciais para fins desta Política, quaisquer informações das partes consideradas não disponível ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, planilhas, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela Mirante e/ou obtidas por meio do exercício das atividades da Mirante.

É importante destacar que todas as informações contidas nos diretórios de rede e bancos de dados da **Mirante Investimentos LTDA** são classificados como estritamente confidenciais e necessitam de sigilo absoluto, devendo ser protegidas de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a utilizá-las e trabalhá-las sempre que necessário.

São exemplos de informações confidenciais:

- Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG etc.), situação financeira e patrimonial e movimentação bancária;
- Informações sobre os fundos que revelem vantagens competitivas em relação ao mercado;
- Todo o material estratégico (impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

As principais diretrizes que devem ser seguidas por todos os colaboradores são as seguintes:

- Informações devem ser tratadas de forma ética e sigilosa, de acordo com as leis e normas vigentes, evitando assim o mau uso, divulgação e exposição.
- A informação deve ser utilizada de forma transparente e para a finalidade para a qual foi obtida exclusivamente.
- A concessão de acessos observa o critério de menor privilégio, ou seja, os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.
- A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.
- Segregação de instalações, equipamentos e informações comuns quando aplicável, com senhas de acesso individuais.

- Senhas devem ser mantidas em segredo pelo colaborador, sendo proibido seu compartilhamento.
- Qualquer ocorrência ou risco de ocorrência, ou identificação de falha na confidencialidade e na segurança da informação devem ser reportados ao responsável pelo Compliance.

Malware

Código malicioso que causa danos ou permite a subversão de sistemas. Exemplos tradicionais de códigos maliciosos incluem vírus, worms, Cavalos de Tróia e scripts de ataque; e os exemplos mais recentes incluem applets maliciosos em Java e controles ActiveX.

Abrangência

Cabe a todos os sócios e Colaboradores assinar o **Termo de Confidencialidade** formalizando a ciência e o aceite da Política de Segurança da Informação e assumindo a responsabilidade pelo cumprimento de suas diretrizes e pela manutenção da confidencialidade das informações.

Todos são igualmente responsáveis por proteger as informações, dentro da limitação de sua respectiva atividade, contra acesso, modificação, destruição ou divulgação não autorizada.

Adicionalmente são definidas as seguintes atribuições específicas relacionadas à Segurança da Informação.

Responsável de Tecnologia da Informação

O sócio Frederico Castro é responsável pela gestão, manutenção e correto funcionamento da infraestrutura responsável por garantir a segurança da informação na **Mirante Investimentos LTDA.**

Além disso, deverá avaliar rotineiramente a infraestrutura e processos, propor iniciativas de melhoria e a alocação de recursos financeiros, humanos e de tecnologia com vistas a garantir a segurança da informação.

Processos e Controles

A Mirante definiu os seguintes processos e controles para garantir a segurança da informação na Mirante Investimentos.

Identificação da Informação

O colaborador que recebe ou prepara uma informação deve identificar a natureza desta. A classificação é realizada de acordo com a confidencialidade e as proteções necessárias, conforme os seguintes níveis: Confidencial, Restrita e Pública. Para a classificação devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

Controles para informações classificadas como "Confidencial"

Informações confidenciais devem ser identificadas como tal: e-mails, apresentações, documentos. Os e-mails e arquivos com informações confidenciais devem ser protegidos e o acesso às informações confidenciais deve ser controlado.

Qualquer documento pessoal que seja disponibilizado a terceiros deve ser enviado com a identificação do terceiro, de preferência editada em marca d'água e sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros.

Controles Gerais de Segurança da Informação e Cibersegurança Salvaguarda da Informação

A informação, ao longo do seu ciclo de utilização e descarte, deve receber proteção adequada, o que inclui desde o momento da Geração, o posterior Manuseio e Armazenamento até o momento final de Descarte.

O colaborador, responsável pela informação gerada, deve ter conhecimento do tempo regulatório de salvaguarda e gerenciar o seu armazenamento e descarte. Na dúvida do tempo regulatório, questionar o Compliance. O descarte de informação confidencial deve ser efetuado utilizando máquina fragmentadora de papéis ou incineradora, no caso de informações digitais, deve haver registro de deleção.

Gestão de Acessos e Vulnerabilidades

A área de Tecnologia da Informação, bom como a figura da pessoa responsável, devem garantir uma adequada Gestão de Acessos que compreende:

- Criar de regras para senhas de acesso aos sistemas corporativos, prevendo inclusive a troca periódica das mesmas quando necessário.
- Todos os perfis de acesso aos sistemas internos e externos de colaboradores, terceirizados e prestadores de serviços, principalmente às informações confidenciais, devem ser criados.
- Controlar o acesso de colaboradores, terceirizados e prestadores de serviços em caso de desligamento e encerramento das atividades.
- Todos os acessos físicos e remotos do ambiente corporativo, inclusive o ambiente de rede, seja por meio de dispositivos corporativos ou pessoais como celulares, devem ser rastreáveis, a fim de garantir que todas as ações sejam passíveis de auditoria e possam identificar, individualmente o Colaborador, para que o mesmo seja responsabilizado por suas ações.
- Os equipamentos, ferramentas e sistemas concedidos aos colaboradores devem ser homologados e configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à política da Mirante.
- Remover de componentes não utilizados e sujeitos a vulnerabilidades;
- Proceder com o bloqueio para instalação de software não padrão;
- Implementar soluções para proteção contra malware configuradas para que monitorem continuamente os sistemas e arquivos de computador e identifiquem características da presença ou atividade de malwares;
- Mecanismos para detectar acessos não autorizados a redes e serviços de rede.

Controles de Segurança Física e Controles de Acesso às Instalações, que devem ser garantidos pela área Administrativa:

- Controle de acesso por meio de crachás e filmagens.
- Espaço físico adequado e restrição de acesso para a guarda de equipamentos e informações confidenciais.

Gestão de Risco e Violações

Parte fundamental da Gestão de Risco diz respeito, em primeiro lugar, a uma avaliação de riscos acompanhada da implementação de controles levando em consideração o ambiente, as atividades, processos e os clientes da Mirante. A avaliação de riscos deve ser atualizada anualmente junto com esta Política de forma a identificar novos riscos, ativos e processos.

A adequada gestão deve contemplar não só o monitoramento, mas também a realização de testes periódicos com o objetivo de detectar as ameaças e reforçar os controles.

Os pontos identificados como de alto controle e confidencialidade já possuem um plano de atuação para tratamento e recuperação de incidentes, incluindo um plano de comunicação.

As violações a esta política devem ser comunicadas imediatamente aos sócios Andre Facury e Frederico Castro e devem ser investigadas para determinação de medidas necessárias à correção da falha e reestruturação de processos. Além disso, medidas devem ser tomadas para evitar que incidentes de segurança se espalhem, para proteger o Banco contra futuras exposições a incidentes similares e para verificar a propagação de incidentes.

Tais medidas de recuperação e resolução devem constar do registro do incidente ou violação.

As violações a esta política estão sujeitas às sanções disciplinares previstas nas normas internas da empresa e na legislação vigente no Brasil.

Backups, Plano de Contingência e Continuidade de Negócio

Com uma periodicidade mínima de 1 ano, o Plano de Contingência e de Continuidade dos principais sistemas e serviços são testados, o objetivo é reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Os mesmos controles de segurança e controle de acesso devem ser aplicáveis nas instalações do site de contingência.

A Mirante possui uma política definida backups diários, com idade histórica semanal, mensal e anual de todas as informações e dados da empresa. Tal backup é realizado em 2 ambientes, o primeiro em HD adicional interno e outro em ambiente de nuvem (Microsoft Azure). Tais backups são testados anualmente.

Testes e Controles

Testes e controles periódicos são realizados com o objetivo de testar efetividade da política de Confidencialidade e Segurança da Informação
O plano de teste é efetuado pelo responsável por Tecnologia da Informação assegurando:

- recursos humanos e computacionais adequados ao porte e às áreas de atuação;
- adequado nível de confidencialidade e acessos as informações confidenciais
- segregação física e lógica
- recursos computacionais, de controle de acesso físico e lógico, estejam protegidos
- manutenção de registros que permita a realização de auditorias e inspeções.

Treinamento

Os colaboradores que têm acesso a informações confidenciais ou participam de processo de decisão de investimento são treinados a respeito de Segurança da Informação. Todos os demais colaboradores são treinados em Cibersegurança.

Tais treinamentos podem incluir:

- Videoaulas
- Testes de Simulação
- Conversas e Palestras
- Documentos e Comunicação Corporativa.