Política de Segurança, Integridade e Confidencialidade da Informação

Aprovada em Conselho de Administração, em 26 de fevereiro de 2021

GRUPO MARQUES

ÍNDICE

1. REGISTO DE APROVAÇÃO E ATUALIZAÇÕES

Tipo de Documento	Políticas Internas
Responsável	Compliance
Nível de Aprovação	Conselho de Administração

Versão	Descrição	Data de Aprovação
1	Versão Inicial	26/02/2021

2. INFORMAÇÃO INSTITUCIONAL

- **Denominação:** MARQUES, S.A. (adiante abreviadamente designada "Marques")
- **Sede:** Rua Joaquim Marques, n.º 34, 9600-049 Pico da Pedra
- **Natureza Jurídica:** Sociedade anónima
- **N.º de Pessoa Coletiva e Matrícula na C.R.C. de Ribeira Grande:** 512 005 761
- **Capital Social:** € 5.500.000,00
- **Entidade Reguladora:** IMPIC, IP

3. ENQUADRAMENTO

A Política de Segurança, Integridade e Confidencialidade de Informação da Marques, S.A., adiante abreviadamente designada “Marques” destina-se a estabelecer os requisitos e princípios a observar no que diz respeito à proteção da informação a que a Marques tem acesso no desenvolvimento da sua atividade.

A informação é um bem tão importante como qualquer outro bem da organização, pelo que tem de ser protegida da forma mais apropriada. A segurança da informação protege a informação contra uma multiplicidade de ameaças, sendo obtida através da implementação de um conjunto de controlos que podem ser: políticas, normas, procedimentos, estruturas organizacionais e funções de software.

A segurança da informação tem como principais objetivos garantir os níveis adequados de integridade, autenticidade, disponibilidade e confidencialidade, requeridos para a sua proteção, mitigando assim o impacto de eventuais incidentes que possam comprometer o regular funcionamento da Marques.

A integridade consiste na capacidade de prevenir, recuperar e reverter alterações não autorizadas ou acidentais aos dados.

A autenticidade consiste na manutenção da fiabilidade da informação desde o momento da sua produção e ao longo de todo o seu ciclo de vida.

A disponibilidade refere-se à possibilidade de acesso aos dados, quando necessário.

A confidencialidade refere-se à capacidade de proteger os dados daqueles que não estão autorizados a consultá-los, não impedindo o acesso aos mesmos, em tempo útil, de pessoas autorizadas.

Para o cumprimento destes objetivos, a Marques, em conformidade com a legislação e normativos em vigor em matéria de segurança da informação, compromete-se a adotar as melhores práticas nacionais e internacionais.

4. ÂMBITO

A política de segurança da informação aplica-se a todas as pessoas que interagem com a informação sob a responsabilidade da Marques, designadamente, os órgãos sociais, colaboradores e prestadores de serviços, doravante designados “utilizadores”.

A presente política aplica-se a toda a informação sob a responsabilidade da Marques, independentemente do suporte de registo: eletrónico, papel, audiovisual ou outro.

Além do acesso adequado à informação necessária para o desempenho das suas funções, todos os utilizadores devem ter conhecimento desta política, sendo-lhes exigido o respeito pelos controlos de segurança implementados.

5. CARACTERÍSTICAS DA INFORMAÇÃO

O valor da informação é resultado das suas próprias caraterísticas, pelo que, qualquer alteração das suas caraterísticas implicará sempre alteração do seu valor, a qual, normalmente, se traduz numa diminuição de valor.

Há três características essenciais da informação que visam garantir a sua segurança. São elas, a confidencialidade, a integridade e a disponibilidade.

5.1. CONFIDENCIALIDADE

A confidencialidade da informação é a qualidade de prevenir a exposição ou o acesso não autorizado à informação, por parte de indivíduos ou sistemas, assegurando que apenas os que possuem direitos e privilégios de acesso a um particular conjunto de informação é que o poderão fazer. Fala-se neste caso em acesso autorizado, estando este apenas acessível às pessoas credenciadas para o efeito.

A proteção de confidencialidade deve impedir o acesso à informação por aqueles que não têm autorização para o fazer e, quando assim não acontecer, estaremos perante uma falha do sistema traduzido num comprometimento ou falha de confidencialidade.

5.2. INTEGRIDADE

A integridade da informação consiste na preservação da precisão, consistência e confiabilidade das informações e sistemas pelos utilizadores, ao longo do seu ciclo de vida. Existe ameaça à integridade da informação, quando esta está exposta a uma modificação não autorizada, corrupção, danificação ou outra qualquer forma de disrupção do seu estado de autenticidade.

5.3. DISPONIBILIDADE

A disponibilidade da informação está relacionada com a acessibilidade a Sistemas, em tempo útil, sem qualquer interferência ou obstrução e no formato necessário.

A disponibilidade de informação assegura que apenas os utilizadores autorizados têm acesso à informação no tempo e no espaço necessário.

6. CONTEÚDO DA POLÍTICA

A política de segurança da informação da Marques consiste na proteção da informação produzida, armazenada, processada ou transmitida contra a perda de integridade, autenticidade, disponibilidade e confidencialidade.

A Marques compromete-se a desenvolver políticas e procedimentos específicos que respeitem as normas internacionais de referência, auditáveis, que definem os requisitos para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), abrangendo, e, ainda, no Regulamento Geral de Proteção de Dados Pessoais, no que respeita a:

a) Recursos Humanos:

i. Assegurar que todos os utilizadores conhecem, entendem e cumprem as responsabilidades na área da segurança da informação em conformidade com as suas funções;

ii. Assegurar que os interesses da Marques e dos utilizadores são protegidos como parte do processo de início, mudança ou cessação de funções;

b) Gestão da Informação:

i. Identificar a informação da Marques e definir as responsabilidades pela sua proteção;

ii. Definir a política de classificação de segurança, assegurando que a informação receba um nível adequado de proteção de acordo com o seu valor, sensibilidade, criticidade, requisitos legais e riscos a que possa estar sujeita;

iii. Definir a política de uso aceitável que deve conter regras para a utilização dos recursos da Marques, ficando o uso destes condicionado à concordância expressa por parte de cada utilizador;

iv. Definir os procedimentos para a gestão dos suportes de armazenamento e salvaguarda da informação;

v. Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação;

c) Gestão de Acessos:

i. Assegurar a gestão e o controlo dos acessos às instalações da Marques, ao sistema informático e à informação, responsabilizando os utilizadores pela proteção das suas credenciais de acesso e assegurando a intransferibilidade dos direitos atribuídos;

ii. Gerir a divulgação da informação;

d) Segurança Física e Ambiental

i. Proteger as informações, equipamentos e instalações físicas da Marques de acesso não autorizado, dano, interferência, perda, furto ou roubo;

ii. Monitorizar e controlar o ambiente das instalações;

iii. Definir procedimentos que assegurem a salvaguarda dos suportes físicos;

e) Gestão do Sistema Informático:

i. Garantir a operação e proteção, segura e correta, dos recursos de processamento da informação;

ii. Registar e monitorizar eventos e gerar evidências;

iii. Analisar, controlar, mitigar e eliminar as vulnerabilidades;

iv. Criar mecanismos que permitam controlar e auditar a conformidade das operações com as políticas de segurança da informação;

v. Garantir a segurança da informação transmitida dentro da organização e com quaisquer entidades externas;

vi. Assegurar o uso efetivo e adequado da criptografia para proteger a integridade, autenticidade e integridade da informação;

f) Gestão dos Incidentes de Segurança: Definir as responsabilidades e os procedimentos a adotar para reagir de forma apropriada perante as fragilidades e incidentes que coloquem em risco a segurança da informação, garantindo o seu registo e prevendo um processo de melhoria contínua e revisão periódica dos processos de gestão de incidentes;

g) Gestão da Continuidade de Negócio

i. Garantir que, após a ocorrência de desastres ou falhas de segurança (resultantes, por exemplo, de desastres naturais, acidentes, falhas de equipamentos ou ações intencionais), seja possível manter um nível de funcionamento aceitável até se retornar à situação normal;

ii. Prever e implementar um plano de continuidade de negócio;

h) Conformidade Legal: Assegurar o cumprimento das obrigações legais, estatutárias, regulamentares e contratuais, bem como de quaisquer requisitos de segurança;

i) Proteção de Dados Pessoais:

i. Identificar e localizar a informação que contem dados pessoais, o seu propósito, risco e valor;

ii. Garantir que os procedimentos a estabelecer sejam adequados às obrigações de proteção de dados pessoais decorrentes, nomeadamente, do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, sobre a proteção de dados pessoais, e legislação nacional aplicável.

7. PRINCÍPIOS APLICÁVEIS

As políticas de segurança da informação da Marques, quer na sua definição, quer na sua concretização diária, devem orientar-se pelos seguintes princípios:

7.1. GARANTIA DE PROTEÇÃO

A informação é um recurso crítico para o eficaz desenvolvimento de todas as atividades da Marques, sendo assim fundamental garantir a sua adequada proteção, nas vertentes de integridade, autenticidade, disponibilidade e confidencialidade.

7.2. SUJEIÇÃO À LEI

A execução da atividade da Marques está sujeita à legislação aplicável, bem como às normas e regulamentos internos.

7.3. NECESSIDADE DE ACESSO

O acesso à informação deve restringir-se, exclusivamente, às pessoas que tenham necessidade de a conhecer para cumprimento das suas funções e tarefas.

7.4. TRANSPARÊNCIA

Deve assegurar-se a transparência, conjugando o dever de informar com a fixação, de forma clara, das regras e procedimentos a adotar para a segurança da informação sob a responsabilidade da Marques.

7.5. PROPORCIONALIDADE

As atividades impostas pela segurança da informação devem ser proporcionais aos riscos a mitigar e limitadas ao necessário, minimizando a entropia no regular funcionamento da Maeques.

7.6. OBRIGATORIEDADE DE CUMPRIMENTO

As políticas e procedimentos de segurança definidos devem ser integrados nos processos de trabalho e a execução das tarefas diárias deve ser pautada pelo seu cumprimento.

7.7. RESPONSABILIDADE

A responsabilidade e o papel das entidades intervenientes na segurança da informação devem ser definidas de forma clara e ser alvo de monitorização.

7.8. INFORMAÇÃO

Todas as políticas e procedimentos específicos devem ser publicitados e comunicados a todos os utilizadores que deles necessitem para o desempenho das suas funções e tarefas.

7.9. FORMAÇÃO

Deve ser planeado, aprovado e executado um plano de formação e de divulgação que incida sobre o domínio da segurança da informação e sobre as políticas e procedimentos específicos adotados neste âmbito.

7.10. AVALIAÇÃO DO RISCO

Deve ponderar-se a necessidade de proteção da informação em função da sua relevância e das ameaças que sobre ela incidem. A avaliação do risco deve identificar, controlar e eliminar os diversos tipos de ameaças a que a informação se encontra sujeita. Os níveis de segurança, custo, medidas, práticas e procedimentos devem ser apropriados e proporcionais ao valor e ao nível de confiança da informação.

7.11. COMUNICAÇÃO, REGISTO E PONTO DE CONTACTO ÚNICO

Todos os incidentes de segurança, bem como as fragilidades, têm de ser objeto de comunicação imediata e registo de forma a proporcionar uma resposta célere aos problemas. O processo de registo deve prever a identificação de um ponto único de contacto para onde devem ser canalizados todos os relatos.

7.12. SANÇÕES

A não observância das disposições de segurança da informação que se encontrem em vigor, será considerada como infração às normas e regulamentos internos e, como tal, será sujeita a medidas corretivas apropriadas de acordo com a legislação e normativos aplicáveis, ou que para o efeito venham a ser estabelecidos.

8. RESPONSABILIDADE

Todos os utilizadores estão obrigados a cumprir e a fazer cumprir a presente política de segurança da informação e têm o dever de zelar pela sua proteção e de proceder à comunicação de qualquer evento que provoque, ou possa provocar, uma quebra de segurança da informação.

O Conselho de Administração da Marques é o primeiro responsável pela implementação e controlo do Sistema de Gestão da Segurança da Informação, competindo-lhe aprovar a presente Política, assim como a “Política de Proteção de Dados Pessoais» e outras Políticas que venham a ser implementadas no âmbito da segurança da informação.

O Conselho de Administração deve ainda garantir que sejam atribuídas as autoridades e responsabilidades para as funções da gestão da informação e para o cumprimento das obrigações legais aplicáveis.

Todos os utilizadores devem cumprir as políticas, regulamentos e procedimentos relativos à segurança da informação.
Os colaboradores de terceiras entidades que prestam serviço na Marques, ou que utilizam as suas instalações e meios, ou ainda os trabalhadores ou empresas contratadas pela Marques, devem cumprir os normativos e procedimentos estipulados na política de segurança da informação.

O Administrador de Segurança, é responsável pelas tarefas de implementação, manutenção e operação do sistema, devendo assegurar, designadamente, a gestão de incidentes de segurança, a execução periódica do processo de avaliação dos riscos de segurança, a elaboração dos planos de formação relativos à segurança da informação e a prestação de apoio às equipas técnicas das especialidades integradas nos processos abrangidos pelo sistema.

O Encarregado da Proteção de Dados é responsável pela aplicação e controlo da legislação relativa à proteção de dados pessoais, nomeadamente nos termos da legislação aplicável, sendo designado com base nos seus conhecimentos especializados no domínio das práticas de proteção de dados, bem como na capacidade para desempenhar as funções legalmente exigidas.

9. MEDIDAS DE CONTROLO, ACOMPANHAMENTO E REPORTE

Qualquer incumprimento dos procedimentos de controlo interno deve ser reportado ao Compliance Officer, com conhecimento do Órgão de Administração ou, diretamente a este órgão quando as circunstâncias o imponham. O reporte deve ser realizado por escrito, sob qualquer forma.

Todas as situações de incumprimento reportadas serão registadas, por um prazo mínimo de cinco anos, e a informação devidamente centralizada de forma a permitir tirar conclusões quanto à eficiência do sistema de controlo das políticas de segurança e implementação das necessárias correções.

Os documentos de reporte de incidentes são conservados em arquivo informático exclusivamente afeto ao seu armazenamento, cuja organização cabe ao Compliance Officer.

No acompanhamento e controlo da aplicação da presente Política deverão ter lugar testes de despiste nomeadamente pela seleção aleatória de um conjunto de colaboradores cujo comportamento no que respeita o cumprimento dos princípios aqui apresentado serão observados. Esta avaliação deverá ocorrer sempre que justificado.

No que respeita a informação qualificada como sensível, de acordo com critérios de razoabilidade, vigora uma política de cautela acrescida que se traduz:

I. Dever de comunicação hierárquica da qualificação de determinada informação como sensível e da importância da sua preservação, aplicação da política de cuidado acrescido;

II. Delinear o elenco de pessoas cuja atividade justifica o acesso à informação, sob pena de prejuízo para o exercício das suas funções; e

III. Utilização exclusivamente para a legítima finalidade.

9.1 CIRCULAÇÃO DE INFORMAÇÃO

Com vista a minimizar o risco de ocorrência de quebras de confidencialidade e da integridade da informação, a Marques adota, na sua organização interna, as medidas necessárias para que as informações de que as pessoas responsáveis pela sua administração e fiscalização ou o seu pessoal hajam tomado conhecimento, em virtude do exercício das suas funções, fiquem limitadas aos serviços e às pessoas diretamente envolvidas nas operações em causa, competindo aos destinatários desta Compilação abster-se de adotar qualquer conduta que possa não ser conforme com a obtenção deste resultado.

O nível de acesso à informação pelas diferentes pessoas envolvidas nas operações será o adequado à responsabilidade das funções desempenhadas, podendo existir, caso se mostre necessário no caso concreto, uma segregação ou compartimentação da informação acessível pelas diferentes pessoas ou áreas envolvidas, por forma a assegurar um controlo interno da informação consentâneo com a natureza da atividade ou da operação em causa. Caberá ao Órgão de Administração a definição dos acessos e canais de informação a que cada colaborador ou parte na operação tenha acesso, tendo em conta as especificidades e a dimensão da operação em concreto.

9.2 SEGREDO PROFISSIONAL

Todas as informações de que os destinatários desta Compilação venham a ter conhecimento no exercício das suas funções estão sujeitas a segredo profissional e ao regime jurídico aplicável às informações privilegiadas, competindo àqueles assegurar, a todo o tempo, rigoroso sigilo profissional sobre todas as informações acima mencionadas.

Os deveres de sigilo estabelecidos no número anterior continuarão a vigorar mesmo após o termo das funções exercidas na Marques e independentemente do motivo por que ocorra, incidindo sobre as informações obtidas ao longo da colaboração estabelecida com a Sociedade.

As informações confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida.

Para os fins desta política, serão consideradas confidenciais todas as informações, transmitidas por meios escritos, eletrónicos, verbais ou quaisquer outros e de qualquer natureza, incluindo, mas não se limitando a: know-how, técnicas, design, especificações, desenhos, cópias, modelos, fluxogramas, croquis, fotografias, software, contratos, planos de negócios, propostas comerciais, processos, tabelas, projetos, nomes de clientes, de revendedor e distribuidor, de colaboradores, resultados de pesquisas, invenções e ideias, financeiras, comerciais, dentre outros.

9.3 RELAÇÕES COM TERCEIROS

A atividade dos destinatários desta Compilação deve pautar-se pelos mais elevados níveis de competência, diligência e eficiência possíveis.

A todos os destinatários desta Compilação incumbe ainda um dever geral de cumprir e de assegurar o cumprimento das regras e princípios nela estabelecidos. Assim, a todos os destinatários é exigível uma conduta com terceiros que transponha, no que seja aplicável, os deveres e obrigações dispostos nesta Compilação, mormente aqueles que digam respeito a deveres de conduta, diligência e segredo.

Cumprirá ao Órgão de Administração, coadjuvado pelo Compliance Officer, sem prejuízo de outras consequências que resultem de lei ou regulamento, monitorizar a conduta dos destinatários para efeitos do cumprimento dos deveres suprarreferidos.

9.4 EXPOSIÇÃO A AMEAÇAS E FALHAS

O sistema pode ser afetado por falhas decorrentes do seu errado manuseamento por parte dos colaboradores ou, ao nível do próprio software por força de falhas técnicas do próprio sistema.

Tais situações devem ser imediatamente reportadas, de modo a que as falhas sejam solucionadas com a maior rapidez possível, sob pena de exposição da informação.

A utilização do sistema informático importa riscos associados quer à utilização humana quer aos vícios do programa e dos equipamentos. Neste contexto, são várias as ameaças como, por exemplo, a exposição a vírus, ou outras formas de fraude informática.

Para diminuir a margem de risco a Sociedade deve implementar todos os mecanismos adequados, devendo para tal efeito consultar técnicos especializados na área. Tenha-se em consideração a importância da implementação de um sistema antivírus com capacidade suficiente. A atualização destes programas será confirmada periodicamente e sempre que se revele necessário. De modo, a compreender e combater acessos externos ao sistema os dados da aplicação dos programas de

combate a ameaças externas devem ser cuidadosamente analisados e tomados em consideração, sendo o tráfico filtrado e, devidamente, monitorizado.

Por constituir fonte de risco acrescido, o acesso remoto deve ser concedido apenas quando necessário e os colaboradores devem ser, especialmente, alertados para a importância de uma utilização prudente.

10 ENTRADA EM VIGOR E REVISÃO

A presente Política entrará em vigor após a sua aprovação pelo Conselho de Administração. Qualquer alteração à mesma terá igualmente de ser objeto de aprovação do Conselho de Administração.

11 DIVULGAÇÃO

A Política de Segurança, Integridade e Confidencialidade da Informação da Marques foi distribuída a todos os colaboradores e órgãos sociais e encontra-se disponível para consulta de qualquer interessado em www.marquessa.pt.