brighten
simplify your business.
together.

POLITICA GERAL SEGURANÇA INFORMAÇÃO (PGSI).

A.5_ Politicas Segurança da Informação

Code/Unit: A05.002	**Type**: Digital
Confidentiality: Publico	**Available on:** Microsoft Teams / Sharepoint

Brighten entidade certificada em ISO/IEC 27001

Version Control

Date	Version	created / edited by	Update Description	Approved (A) by: Date:
Dez 2020	V1.0	SB	Documento Base	A: Managing Partner Data: Dez 2020
Fev 2021	V1.1	SB	Atualização do ponto objetivos	A: Managing Partner Data: Fev 2021
Dez 2021	V1.2	SB	Atualização de template	A: Managing Partner Data: Dez 2021

Index

1. INTRODUÇÃO 4
1.1. Objetivo 4
1.2. Âmbito e Utilizadores 4
2. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO 4
3. OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 6
4. LINHAS ORIENTADORAS PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO 6
5. ATRIBUIÇÃO DE RESPONSABILIDADES 9
6. ENTRADA EM VIGOR E REVISÃO 10

1. INTRODUÇÃO

O presente documento faz parte integrante da Politica de Segurança de Informação da **Brighten S.A.** (doravante designada por "Entidade", "Organização" ou "Brighten"), estando enquadrado no Sistema de Gestão de Segurança de Informação (SGSI).

1.1. Objetivo

Na **Brighten**, a informação é vista como um ativo crítico e fundamental, pelo que a Gestão da Brighten considera estratégica a definição e aplicação de uma política geral que salvaguarde a integridade, disponibilidade e confidencialidade da informação, no sentido de a proteger de forma adequada, assegurando a **melhoria contínua e a continuidade e eficácia do negócio**.

Esta política destina-se a todas as partes interessadas e tem como objetivo identificar os princípios de Segurança da Informação que deverão ser seguidos na **Brighten**, bem como definir as linhas orientadoras de segurança da Informação e os respetivos objetivos de controlo.

1.2. Âmbito e Utilizadores

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

Neste contexto, a presente política aplica-se a todos os funcionários da **Brighten**, pessoal temporário, prestadores de serviços, consultores, parceiros e terceiros (doravante designados por "colaboradores" ou "utilizadores") que interagem com a informação sob a responsabilidade da **Brighten**.

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

2. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

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

1. *Proteção e Classificação da Informação* - assegurar a proteção e classificação da informação e dos seus ativos de suporte nas vertentes de integridade, autenticidade, disponibilidade e confidencialidade;

2. *Conformidade legal* - tanto a política como as tarefas executadas no seu âmbito estão sujeitas à legislação aplicável, bem como às normas e regulamentos internos

relativos à informação aprovados pela Gestão, requisitos de clientes e outros externos à organização;

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;

4. *Transparência e Responsabilidades* – assegurar 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 **Brighten**. As responsabilidades e o papel dos intervenientes na segurança da informação devem ser definidas de forma clara e ser alvo de monitorização e auditoria periódicas;

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 **Brighten**;

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. *Informação* - todas as políticas e procedimentos específicos devem ser publicitados e comunicados a todos os colaboradores que deles necessitem para o desempenho das suas funções e tarefas;

8. *Formação* - deve ser planeado, aprovado e executado um plano de divulgação e de formação dos colaboradores, que incida sobre o domínio da segurança da informação e sobre as políticas e procedimentos específicos adotados neste âmbito;

9. *Gestão de Incidentes de Segurança* – efetuar uma adequada gestão de incidentes de segurança, através de processos de prevenção, deteção, registo, comunicação, tratamento e investigação dos incidentes e das vulnerabilidades que possam comprometer a segurança da informação, a proteção dos dados pessoais ou interromper a continuidade do negócio. O processo de registo deve prever a identificação de um ponto único de contacto para onde devem ser canalizados todos os relatos;

10. *Melhoria Continua* – Melhorar de forma continua a aplicabilidade, adequabilidade e eficácia do SGSI e incorporar a Segurança da Informação nos processos e

objetivos de negócio da Brighten, como condição necessária à satisfação e confiança dos clientes, e como fator diferenciador e competitivo.

3. OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação tem como principais objetivos proteger a informação e os seus ativos de suporte, garantindo os níveis adequados de integridade, autenticidade, disponibilidade e confidencialidade, mitigando assim o impacto de eventuais incidentes que possam comprometer o regular funcionamento da Brighten:

- 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, sempre que 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 **Brighten**, 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. LINHAS ORIENTADORAS PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Por **Informação**, a **Brighten** entende tratar-se de qualquer fluxo de comunicação ou representação de conhecimento como dados, factos ou opiniões, em qualquer meio ou formato.

Por **Ativo de Informação**, a **Brighten** entende tratar-se de qualquer ativo que suporta informação, em qualquer formato, e que possui um valor intrínseco para a organização. Os ativos incluem as próprias entidades de informação (como base de dados, contratos etc), o hardware (i.e. computadores, equipamentos de redes de comunicações etc), o software (i.e. aplicações, sistemas operativos, plataformas de rede, etc), os serviços, as pessoas (i.e conhecimento, qualificações, etc) entre outros.

Por **Segurança da Informação**, a Brighten entende tratar-se da proteção da informação e dos seus ativos de suporte, de um amplo conjunto de ameaças através de um processo de gestão de riscos, garantindo a continuidade de negócio.

Neste sentido, a **Brighten** 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, nomeadamente as áreas previstas da norma ISO/IEC 27001:2013, e, ainda, no Regulamento Geral de Proteção de Dados Pessoais – Regulamento (UE) 2016/679, em concordância com os objetivos estratégicos da organização no que respeita a:

- ***Segurança dos Recursos Humanos*** - Assegurar que todos os colaboradores conhecem, entendem e cumprem as responsabilidades na área da segurança da informação em conformidade com as suas funções. Assegurar a adoção de controlos que visam proteger os interesses da **Brighten** e dos colaboradores relacionados com processos de início, mudança ou cessação de funções;

- ***Gestão da Informação e Comunicação*** - Identificar a informação da **Brighten** e definir as responsabilidades pela sua proteção, incluindo a definição da Política de Gestão da Informação, 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. Assegurar a gestão operacional e utilização segura dos ativos TIC que suportam os utilizadores finais, e ainda à proteção adequada da informação em alguns processos específicos de comunicação e transferência dentro e fora da organização, garantindo que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação;

- ***Segurança e Operação dos Sistemas e Instalações*** – definição de objetivos de segurança fisíca e lógica a aplicar aos sistemas e instalações, nomeadamente:
    - *Gestão de Acessos* – gerir a divulgação da Informação e assegurar a gestão e o controlo dos acessos às instalações da **Brighten**, ao sistema informático e à informação, responsabilizando os utilizadores pela proteção das suas credenciais de acesso e assegurando a intransferibilidade dos direitos atribuídos;
    - *Segurança Física e Ambiental* - proteger as informações, equipamentos e instalações físicas da **Brighten** contra o acesso não autorizado, dano, interferência, perda, furto ou roubo, bem como monitorizar e controlar o ambiente das instalações, pela definição de procedimentos que assegurem a salvaguarda dos suportes físicos;
    - *Gestão do Sistema Informático* – garantir a operação e proteção, segura e correta, dos recursos de processamento da informação; Registar e

monitorizar eventos e gerar evidências; Analisar, controlar, mitigar e eliminar as vulnerabilidades; Criar mecanismos que permitam controlar e auditar a conformidade das operações com as políticas de segurança da informação; Garantir a segurança da informação transmitida dentro da organização e com quaisquer entidades externas; Assegurar o uso efetivo e adequado da criptografia para proteger a integridade, autenticidade e integridade da informação;

- ***Gestão dos Incidentes de Segurança*** - definir as responsabilidades e os procedimentos a adotar para reagir de forma apropriada perante incidentes de segurança, incluíndo a deteção, a resposta, e o reporte e comunicação de incidentes, garantindo o seu registo e prevendo um processo de **melhoria continua e revisão periódica dos processos de incidentes**;

- ***Gestão dos Riscos de Segurança*** – definir o modelo de governança ('*governance*') da organização relativamente à segurança, incluindo a definição de papeis e responsabilidades de segurança, bem como, as metodologias para gestão e avaliação de riscos de segurança (incluindo a identificação, controlo e eliminação dos diversos tipos de ameaças a que a informação se encontra sujeita). Definição dos requisitos de segurança para a gestão de terceiros, de acordo com os requisitos de negócio, de clientes e regulamentação aplicável;

- ***Gestão da Continuidade de Negócio*** – objetivos de segurança que visam garantir a estratégia de continuidade e aos planos de continuidade e de gestão de crise, para mitigar falhas de segurança com impacto significativo na organização (resultantes, por exemplo por desastres naturais, acidentes, falhas de equipamentos ou ações intencionais), mantendo um nível de funcionamento aceitável até se retornar à situação normal;

- ***Monotorização e Auditoria*** – objetivos de segurança relativos aos processos de *logging*, monotorização e auditorias de segurança às redes, sistemas de informação e instalações da organização com vista à **melhoria continua do SGSI**;

- ***Conformidade Legal*** - assegurar o cumprimento das obrigações legais, estatutárias, regulamentares e contratuais, bem como de quaisquer requisitos de segurança, incluindo a Proteção de Dados Pessoais, nomeadamente:
    - Identificar e localizar a informação que contém dados pessoais, o seu propósito, risco e valor, garantindo, 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.

5. ATRIBUIÇÃO DE RESPONSABILIDADES

As responsabilidades e autoridades específicas no âmbito de Gestão da Segurança da Informação são detalhados no documento "*SI_Manual de Gestão da Segurança da Informação*".

Adicionalmente, a Gestão da **Brighten** é a primeira responsável pela implementação e controlo do Sistema de Gestão da Segurança da Informação (SGSI), competindo-lhe aprovar os documentos «Política de Gestão da informação», «Política de proteção de dados pessoais» e outras Políticas definidas na sequência da implementação do Sistema de Gestão de Segurança da Informação (SGSI). A Gestão, deve também garantir que sejam atribuídas as autoridades e responsabilidades para as funções da gestão da informação e para o cumprimento das obrigações legais aplicáveis, bem como representar o compromisso para com a Segurança da Informação.

Os colaboradores (incluindo a gestão de topo e todos aqueles que fazem parte da estrutura organizacional de Gestão de Segurança da Informação) têm a responsabilidade de manter um comportamento responsável e consistente com "**Objetivos de Segurança da Informação**". Para tal, os utilizadores devem conhecer as instruções (incluindo Políticas e procedimentos), regras e penalidades de funcionamento, devendo ainda:

- Aceitar plenamente as regras e responsabilidades definidas neste documento e de normas e procedimentos internos da **Brighten** sobre a utilização dos recursos de tratamento da informação;
- Cumprir com os códigos de ética profissional, bem como com os requisitos da legislação em vigor relacionados com as atividades da **Brighten**, incluindo com a legislação em vigor de proteção de dados pessoais;
- Responder por atos que violem as regras de utilização dos recursos computacionais, estando, portanto, sujeito às penalidades definidas na política de uso desses recursos e também, se for o caso, às penalidades impostas pela legislação em vigor;
- Comunicar imediatamente qualquer falha ou não conformidade identificada na Segurança da Informação de acordo com o procedimento de notificação de incidentes;
- Não se fazer passar por outra pessoa ou dissimular sua identidade enquanto a utilizar os recursos da organização;
- Responsabilizar-se pela sua identidade eletrónica, passwords, credenciais de autenticação, autorização ou outro dispositivo de segurança, não partilhando com ninguém esta informação;

- Responder pela utilização indevida da sua conta e dos recursos computacionais em qualquer circunstância;
- Divulgar informação interna e/ou confidencial apenas nas situações previstas na lei, devendo, para tal efeito, recorrer a aconselhamento deontológico e jurídico (Comissão de Ética e Responsável do Acesso à Informação).

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.

6. ENTRADA EM VIGOR E REVISÃO

A presente política geral de segurança da informação entra em vigor na data da sua publicação e será revista sempre que seja considerado necessário.