Política de Segurança da Informação

28.mar.2023

Índice de Versões

22.Abr.2015
Versão Inicial

21.Mai.2019
Revisão Geral

22.nov.2022
Revisão Geral

28.mar.2023
Inclusão de referência ao Regulamento (UE) 2016/1011 do Parlamento Europeu e do Conselho de 8 de junho de 2016. Ajustado o texto do ponto 3.2.. Acrescentado o Gestor de Segurança da Informação no capítulo 3.

Introdução

O OMIP, enquanto Operador de Mercado Regulamentado tal como definido no artigo 4 (1) da Directiva 2014/65/EU do Parlamento Europeu e do Conselho, de 15 de Maio de 2014 (MIFID II), tem a preocupação constante de estar dotado de um amplo conjunto de ferramentas de gestão da segurança da informação, de forma a garantir que os seus sistemas de tecnologia de informação e o quadro de segurança da informação estão em conformidade com os padrões, referências e normas internacionais e ainda com os requisitos legais, nomeadamente, com:

- Regulamento (UE) n.º 1227/2011 do Parlamento Europeu e do Conselho, de 25 de Outubro de 2011, relativo à integridade e à transparência nos mercados grossistas de energia (REMIT);
- Regulamento de Execução (UE) N.º 1348/2014 da Comissão de 17 de Dezembro de 2014 relativo à comunicação de dados que dá execução ao artigo 8.º, n.º 2 e 6, do Regulamento (UE) n.º 1227/2011 do Parlamento Europeu e do Conselho relativo à integridade e à transparência nos mercados grossistas da energia;
- Directiva de Mercados 2014/65/EU (MiFID II) do Parlamento Europeu e do Conselho, de 15 de Maio de 2014, relativo aos mercados de instrumentos financeiros, que emenda a Directiva 2002/92/EC e Directiva 2011/61/EU, e respectivas normas de nível inferior;
- Regulamento (EU) nº 600/2014 (MiFIR), do Parlamento Europeu e do Conselho, aprovado a 15 de Maio de 2014, relativo aos mercados e instrumentos financeiros, que emenda a Regulação (EU) Nº 645/2012, e respectivas normas de nível inferior;
- Regulamento (UE) 2016/1011 do Parlamento Europeu e do Conselho de 8 de junho de 2016, relativo aos índices utilizados como índices de referência no quadro de instrumentos e contratos financeiros ou para aferir o desempenho de fundos de investimento (RIR).

A segurança da informação é definida pelas práticas que permitem assegurar que a informação sob responsabilidade de uma organização apenas é acedida ou modificada, durante o seu armazenamento, processamento ou transmissão, pelas pessoas, entidades ou sistemas autorizados. Estas práticas incluem as medidas necessárias para detetar, documentar e responder às ameaças à integridade, disponibilidade e confidencialidade da informação.

Toda a informação tem um valor associado, em alguns casos diretamente convertível em valor monetário, noutros associado a fatores qualitativos, nomeadamente reputacionais. A quebra da sua confidencialidade, integridade ou disponibilidade, no tratamento pelos seus utilizadores, pode implicar perdas significativas para a organização.

Atento a estes fatores, o OMIP estabelece, através da presente Política de Segurança da Informação, os alicerces da sua organização na gestão da segurança da informação, visando atingir os seguintes objetivos:

- **Confidencialidade:** garantir que a informação está acessível somente às pessoas ou sistemas autorizados, pelo período necessário;
- **Integridade**: garantir que a informação está completa, íntegra e que não é modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida;
- **Disponibilidade**: garantir que a informação está disponível a todas as pessoas autorizadas, sempre que necessário.

Nesse sentido, encontram-se aqui estabelecidas as principais diretrizes relativas ao Sistema de Gestão de Segurança da Informação (vulgo ISMS) do OMIP, baseado na norma ISO 27001, uma das normas de referência internacional para a gestão da segurança da informação. Este sistema visa proteger a informação sobre a qual o OMIP tem responsabilidade, quer tenha sido produzida internamente, quer

tenha sido confiada no âmbito das funções que desempenha, dos serviços que presta aos seus clientes e das responsabilidades a que se encontra sujeita legal ou regulamentarmente.

1. Âmbito

A presente Política aplica-se aos colaboradores do OMIP, ao Conselho de Administração do OMIP, aos estagiários, prestadores de serviços e outros parceiros, bem como a todos os ativos em operação, inativos ou a desenvolver, quer estejam alojados em equipamentos e instalações do OMIP quer sejam objeto de fornecimento externo.

O âmbito de aplicação desta Política estende-se a todas as áreas de funcionamento do OMIP cuja atuação tem impactos na segurança da infomação.

2. Objetivos

São prosseguidos os seguintes objetivos para salvaguardar a confidencialidade, integridade e disponibilidade de todos os ativos de informação:

a) Assegurar a conformidade com a legislação, regulamentação e demais normas aplicáveis;
b) Cumprir com os requisitos de confidencialidade, integridade e disponibilidade adequados aos objetivos de negócio do OMIP, em particular com as necessidades dos seus membros;
c) Estabelecer controlos para proteger os ativos de informação do OMIP de roubo, intrusão, abuso ou outras formas de tratamento ilícito;
d) Promover uma cultura de sensibilização e compromisso para a segurança da informação entre os membros do Conselho de Administração, a Gestão de Topo e os Colaboradores, motivando-os a tomarem conhecimento e assumirem a responsabilidade pela sua intervenção no ISMS, de forma a minimizar o risco de incidentes de segurança;
e) Assegurar a disponibilidade e fiabilidade dos equipamentos, infraestruturas e sistemas que suportam a atividade do OMIP;
f) Assegurar que o OMIP tem a capacidade de prosseguir a prestação dos seus serviços caso ocorram incidentes de segurança graves, nas condições definidas nas normas e procedimentos específicos aplicáveis;
g) Assegurar a proteção de dados pessoais, de acordo com o previsto na legislação aplicável;
h) Seguir as melhores práticas da indústria, nomeadamente as baseadas na normativa aplicável;
i) Assegurar que os fornecedores externos, nomeadamente os fornecedores críticos, se enquadram nas necessidades e requisitos de segurança do OMIP;
j) Reduzir os danos inerentes à ocorrência de incidentes de segurança da informação no OMIP, assim como garantir que os mesmos são reportados nos termos definidos para o efeito;
k) Assegurar a melhoria contínua do ISMS, de forma a garantir a sua adequação e eficácia.

3. Funções e responsabilidades

3.1 Conselho de Administração

O Conselho de Administração do OMIP detém, em última instância, a responsabilidade global pela segurança da informação e, em particular, pela definição e aprovação da presente Política, bem como

da sua revisão, de forma a garantir a sua contínua adequação e eficácia. A competência na aprovação da restante documentação, incluindo a referente ao ISMS, é delegada no Diretor de Operações, que deverá manter os membros do Conselho de Administração informados e atualizados, de forma regular, das respetivas revisões, dos desenvolvimentos e melhorias no sistema e dos resultados de auditorias, testes e avaliações (internas ou independentes).

3.2 Gestão de Topo

A Gestão de Topo do OMIP, constituída pelo Presidente e Vice-presidente do Conselho de Administração e pelo Diretor de Operações, detém a responsabilidade de apoiar e suportar todas as fases de implementação e manutenção do ISMS, assegurando os recursos adequados e de forma a garantir a concretização dos objetivos definidos na presente Política. É da responsabilidade da Gestão de Topo submeter ao Conselho de Administração, para aprovação, a presente Política e respetivas alterações.

3.3 Comité de Segurança

No âmbito da implementação do ISMS, foi constituído o Comité de Segurança do OMIP, sendo este um comité interno de carácter técnico, composto, pelo menos, pelo Diretor de Operações, por um responsável do departamento de Sistemas de Informação e pelo Gestor de Segurança da Informação. O Comité de Segurança é responsável pela implementação, manutenção e revisão das políticas e procedimentos do ISMS, de acordo com os objetivos e princípios que se encontram definidos na presente Política.

3.4 Gestor de Segurança da Informação

Ao Gestor de Segurança da Informação do OMIP são atribuídas as seguintes funções e responsabilidades:

- Responsável pela implementação e manutenção do ISMS;
- Responsável por efetuar a ligação entre o Comité de Segurança e todas as restantes áreas no âmbito do ISMS;
- Garantir que o ISMS está de acordo com os objetivos de negócio do OMIP, requisitos da ISO 27001:2013 e demais requisitos regulamentares decorrentes da atividade do OMIP;
- Desenvolver e implementar, sempre que necessário, programas de formação e sensibilização para a segurança da informação junto dos colaboradores;
- Garantir que as não conformidades do ISMS são corrigidas no menor espaço de tempo possível;
- Cumprir e assegurar o cumprimento de todos os requisitos, políticas e procedimentos do ISMS.

3.5 Colaboradores

Os colaboradores do OMIP são responsáveis por:

- Cumprir todas as normas, requisitos, políticas e procedimentos definidos no âmbito da segurança da informação;
- Os activos de informação que lhe são confiados, devendo contribuir proactivamente para a devida proteção dos mesmos;
- Reportar a ocorrência de incidentes ou anomalias de segurança da informação no OMIP de acordo com os procedimentos internos definidos para o efeito .

3.6 Fornecedores

Os fornecedores devem adotar condutas e procedimentos consistentes com a presente Política. Em particular, os contratos entre o OMIP e empresas prestadoras de serviços com acesso à informação, aos sistemas e/ou ao ambiente tecnológico do OMIP devem conter cláusulas que garantam a confidencialidade entre as partes e que assegurem que os profissionais sob sua responsabilidade cumpram a presente Política, normas e demais procedimentos que sejam aplicáveis.

Os fornecedores são também responsáveis por reportar ao OMIP a ocorrência de incidentes de segurança da informação do OMIP ou em sistemas de informação do OMIP.

Os fornecedores que sejam considerados críticos para o OMIP devem ser objeto de maior controlo e monitorização, bem como de requisitos de segurança adicionais no âmbito da relação contratual entre as partes.

4. Princípios da Segurança de Informação

4.1 Normas de conduta

O OMIP define normas de conduta relativas à segurança da informação aplicáveis aos seus colaboradores e fornecedores externos, nomeadamente nos seguintes capítulos:

- Cumprimento da presente Política e da demais documentação de segurança da informação;
- Utilização dos recursos tecnológicos e dos sistemas disponibilizados pelo OMIP;
- Tratamento da informação e dados pessoais sob a responsabilidade do OMIP;
- Tratamento dos incumprimentos ou violações da presente Política ou das demais políticas e procedimentos de segurança da informação.

4.2 Recursos humanos

A segurança da informação é aplicável a todos os colaboradores do OMIP em todos os departamentos, de forma transversal, devendo ser atribuídas responsabilidades específicas a determinadas funções. Nesse sentido, o OMIP deve promover a formação e transmitir a informação necessária para que os seus colaboradores, bem como os colaboradores de fornecedores externos, estejam aptos a assumir as suas responsabilidades no âmbito da segurança da informação.

4.3 Gestão de Ativos

A informação gerida pelo OMIP, os seus processos e infraestruturas de suporte, colaboradores, terceiras partes, escritórios, equipamentos, documentos, sistemas, aplicações e redes são ativos valiosos para a organização. Devem ser, por isso, adequadamente protegidos, em conformidade com os procedimentos de segurança da informação aprovados pelo OMIP, em todo o seu ciclo de vida, o qual inclui a sua criação, manuseamento, armazenamento, transporte e destruição.

A informação gerida pelo OMIP deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi gerada ou confiada.

4.4 Sistemas de informação

O armazenamento de informação é maioritariamente realizado em arquivos tecnológicos, pelo que deve ser prestada especial atenção aos procedimentos específicos que gerem os sistemas de informação, bem como os ativos que os suportam.

Os sistemas de informação do OMIP devem ser planeados, especificados, desenvolvidos, testados, implantados e geridos tendo em conta as necessidades e os requisitos de segurança da informação – confidencialidade, integridade e disponibilidade.

4.5 Dados Pessoais

O OMIP assume o compromisso de efetuar todos os esforços para garantir a privacidade e a proteção dos dados pessoais que lhe são confiados, em conformidade com a regulamentação aplicável e, em particular, com o Regulamento Geral sobre Protecção de Dados. O OMIP classifica os dados pessoais como confidenciais, adotando as medidas adequadas de segurança físicas, lógicas, técnicas e organizativas, de forma a proteger os dados pessoais contra a sua difusão, alteração, perda, má utilização, tratamento e acesso não autorizado ou roubo, bem como contra qualquer outra forma de tratamento ilícito.

4.6 Gestão de risco

Uma das áreas fulcrais do ISMS do OMIP é a gestão – identificação, avaliação e tratamento – contínua dos riscos, inerentes à sua atividade, aos quais os ativos da organização se encontram expostos, constituindo uma ferramenta de gestão da empresa. A gestão de risco no âmbito do ISMS inclui a implementação de controlos e mecanismos de segurança que visam mitigar ou limitar os potenciais danos provocados pela exploração das vulnerabilidades dos ativos, de forma a minimizar a ocorrência de incidentes e garantir um nível de segurança adequado face ao risco que o OMIP está disposto a assumir. Estas medidas devem ser definidas de acordo com os objetivos de negócio e as responsabilidades do OMIP, tendo em conta a eficiência, o custo e a sua aplicabilidade.

4.7 Gestão de Incidentes e Continuidade do Negócio

Todos os eventos que possam pôr em causa as operações de negócio ou comprometer a segurança da informação serão tratados como incidentes de segurança, em conformidade com os procedimentos de gestão de incidentes designados pelo OMIP.

A disponibilidade da informação, não descurando a responsabilidade dos restantes compromissos de segurança da informação, será assegurada pela implementação de respostas a incidentes disruptivos e que se integram no âmbito do Sistema de Gestão da Continuidade do Negócio do OMIP.

4.8 Cibersegurança

Estando ciente da importância crescente da cibersegurança como área específica no âmbito da segurança da informação, o OMIP deve desenvolver e aplicar uma Política de Cibersegurança alinhada com as melhores práticas e normas de referência, e que lhe permita cumprir com os requisitos regulamentares aplicáveis em matéria de cibersegurança, nomeadamente os que se aplicam à sua atividade de Operador de Mercado Regulamentado e ainda como operador de serviços essenciais no setor das infraestruturas do mercado financeiro. Adicionalmente, o OMIP deverá estabelecer, sempre que possível, protocolos e processos de cooperação com entidades com funções de autoridade nacional competente em matéria de cibersegurança.

5. Disposições Finais

A presente Política deve ser revista pelo Conselho de Administração sempre que se verifique alguma alteração no âmbito da segurança da informação, na organização interna do OMIP, no enquadramento legal e regulatório ou nas melhores práticas seguidas pela indústria.

A presente Política encontra-se disponível para consulta no seu *site* corporativo.

Aprovado pelo Conselho de Administração em 28 de março de 2023