Política de Segurança da Informação

26.nov.2024

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.

26.nov.2024
Fusão da Política de Segurança da Informação e da Política de Cibersegurança. Revisão geral.

1. 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), e enquanto entidade identificada, pelo Centro Nacional de Cibersegurança, como Operador de Serviço Essencial no setor das Infraestruturas do mercado financeiro, nos termos do n.º 1 do artigo 29.º da Lei n.º 46/2018, tem a preocupação constante de estar dotado de um amplo conjunto de procedimentos de gestão de segurança da informação e de cibersegurança, de forma a garantir que os seus ativos e sistemas e tecnologias de informação e comunicação (TIC) estão em conformidade com os padrões, referências e normas internacionais e ainda com os requisitos legais, nomeadamente:

- 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)Lei n.º 46/2018 (de 13 de Agosto) que estabelece o regime jurídico da segurança do ciberespaço (transpondo a Directiva (UE) n.º 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016);
- Decreto-Lei n.º 65/2021 de 30 de julho que regulamenta o regime jurídico da segurança do ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019;
- Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (Regulamento DORA);
- ISO/IEC 27032:2012;
- ISO/IEC 27001:2013;
- *CIS Controls* v8;
- Quadro Nacional de Referência para a Cibersegurança, Centro Nacional de Cibersegurança (CNCS);
- *Framework for Improving Critical Infrastructure Cybersecurity* (v1.1, April 16, 2018), NIST;

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.

Dentro da segurança da informação, assume especial relevância a área da cibersegurança, definida como a preservação da confidencialidade, integridade e disponibilidade da informação no ciberespaço, ou seja, no espaço não físico criado por redes de computadores, nomeadamente pela Internet, onde as pessoas podem comunicar e interagir por via de *softwares*, plataformas ou outros serviços de 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 e da cibersegurança, visando atingir os seguintes macro 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 (ISMS) do OMIP, baseado na norma ISO/IEC 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.

2. Âmbito

A presente Política aplica-se a todos os colaboradores, incluindo os membros dos órgãos sociais e fornecedores do OMIP.

O âmbito de aplicação desta Política estende-se a todas as áreas de funcionamento do OMIP cuja atuação tenha impactos na segurança da informação e na cibersegurança, e inclui todos os seus ativos tecnológicos em operação, inativos ou em desenvolvimento, quer estejam alojados em equipamentos e instalações do OMIP, quer sejam objeto de fornecimento externo.

3. Objetivos de Segurança da Informação

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

3.1. Assegurar a conformidade com a legislação, regulamentação e demais normas aplicáveis;

3.2. Assegurar a proteção de dados pessoais de acordo com o previsto na legislação aplicável;

3.3. Seguir as melhores práticas da indústria e das referências e normas internacionais de segurança e cibersegurança;

3.4. Promover uma cultura de sensibilização e compromisso para a segurança da informação e para a cibersegurança 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;

3.5. Assegurar a disponibilidade e fiabilidade dos equipamentos, infraestruturas e sistemas que suportam a atividade do OMIP;

3.6. Cumprir com os requisitos de confidencialidade, integridade e disponibilidade adequados aos objetivos de negócio do OMIP, em particular com as necessidades dos seus clientes;

3.7. Assegurar que os fornecedores, nomeadamente os fornecedores cujo serviço prestado sustente uma função crítica ou importante, se enquadram nas necessidades e requisitos de segurança e cibersegurança do OMIP;

3.8. Identificar, avaliar e tratar os riscos de segurança da informação e de cibersegurança inerentes à atividade do OMIP e aos quais os seus ativos se encontram expostos, de acordo com a tolerância ao risco definida pela organização;

3.9. Estabelecer e implementar controlos para proteger os ativos de informação do OMIP em função da sua relevância e criticidade, de forma a que possam ser adequadamente protegidos em todo o seu ciclo de vida, e monitorizar a sua eficácia;

3.10. Identificar, conter e solucionar incidentes de segurança da informação e, em particular, ciberataques, assim como garantir que os mesmos são reportados em conformidade com a legislação em vigor e com os procedimentos internos definidos para o efeito;

3.11. Reduzir os danos no negócio inerentes à ocorrência de incidentes de segurança da informação, assegurando que o OMIP tem a capacidade de prosseguir a prestação dos seus serviços, nomeadamente das suas funções de negócio críticas ou importantes, caso ocorram incidentes de segurança graves, minimizando os impactos negativos que possam advir da ocorrência dos mesmos tanto para o OMIP como para todas as partes interessadas;

3.12. Promover a partilha de informação relevante em matéria de cibersegurança, através de canais seguros e em tempo útil, com as partes interessadas do OMIP, do Grupo OMI, entidades oficiais e outros grupos de interesse, contribuindo para a globalização da consciencialização sobre cibersegurança;

3.13. Promover estratégias de implementação de oportunidades de melhoria, nomeadamente as propostas resultantes de auditorias, testes de intrusão ou de análise de vulnerabilidades, ou outros projetos internos ou externos relevantes em matérias de segurança da informação e de cibersegurança;

3.14. Assegurar a melhoria contínua do ISMS, de forma a garantir a sua adequação e eficácia.

4. Controlos de Segurança

4.1. Normas de Conduta

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

- Cumprimento da presente Política e 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.

4.2. 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 Proteção de Dados. O OMIP classifica os dados pessoais como confidenciais, adotando as medidas adequadas de segurança físicas, lógicas, técnicas e organizativas, incluindo controlos de proteção de exfiltração de dados, 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.

4.3. 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, implementados e geridos tendo em conta as necessidades e os requisitos de segurança da informação – confidencialidade, integridade e disponibilidade.

4.4. 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 relevantes para a organização. São, por isso, devidamente identificados, inventariados, mantidos, classificados e controlados em função dessa mesma importância e criticidade, de forma que possam ser adequadamente protegidos em todo o seu ciclo de vida (o qual inclui a sua criação, manuseamento, armazenamento, transporte e destruição), em conformidade com os procedimentos de segurança da informação e de cibersegurança aprovados pelo OMIP.

4.5. 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 promove ações de formação e sensibilização em segurança da informação e cibersegurança e transmite a informação necessária para que os seus colaboradores (incluindo os membros dos órgãos sociais) e fornecedores estejam aptos a assumir as suas responsabilidades no âmbito da segurança da informação. O OMIP valida posteriormente o sucesso e eficácia destas ações através de campanhas de, por exemplo, simulação de eventos.

Os colaboradores dos departamentos com acessos privilegiados às redes e aos sistemas de informação do OMIP têm, adicionalmente e antes de assumirem funções, formação específica sobre gestão de acessos e demais procedimentos operacionais. Os colaboradores com responsabilidades acrescidas na segurança da informação e cibersegurança do OMIP têm ainda formação especializada nas respetivas áreas.

4.6. Gestão de Fornecedores

Na gestão de fornecedores, em particular dos fornecedores cujo serviço prestado sustente uma função crítica ou importante, o OMIP segue os princípios estabelecidos na sua Política de Gestão de Fornecedores, nomeadamente, a definição dos requisitos de segurança da informação para a mitigação dos riscos associados ao acesso de fornecedores (e da cadeia de fornecimento de tecnologias de informação e comunicação) aos ativos de informação, assim como a manutenção do nível de segurança da informação e de disponibilidade dos serviços prestados em conformidade com as condições contratadas com os fornecedores, através do estabelecimento de procedimentos de monitorização e de avaliação da entrega do serviço por parte de fornecedores.

4.7. Gestão do Risco

Uma das áreas fulcrais do ISMS no OMIP é a gestão – identificação, análise, avaliação e tratamento – contínua dos riscos de segurança da informação e de cibersegurança inerentes à sua atividade, aos quais os ativos da organização se encontram expostos, constituindo uma ferramenta de gestão da empresa. A metodologia de gestão do risco do OMIP, no âmbito do ISMS, envolve:

- Identificação e documentação das ameaças internas e externas que possam explorar as vulnerabilidades dos ativos do OMIP, pondo em causa a integridade, confidencialidade ou disponibilidade dos mesmos;
- Avaliação baseada em cenários de risco, para os quais são aferidos a probabilidade e o impacto, que compõem o nível de risco;
- Tratamento dos riscos, de acordo com a criticidade e os critérios de aceitação e de priorização do risco da organização.

No âmbito do tratamento, a gestão do risco inclui a implementação de controlos e mecanismos de segurança que visam reduzir, transferir, evitar ou aceitar os potenciais danos provocados pela exploração das vulnerabilidades dos ativos, de forma a minimizar os impactos e a ocorrência de incidentes de segurança da informação e garantir um nível de segurança adequado face ao risco que o OMIP está disposto a assumir. Estas medidas são definidas de acordo com os objetivos de negócio e as responsabilidades do OMIP, tendo em conta a eficiência, o custo e a sua aplicabilidade.

4.8. Gestão de Incidentes

Todos os eventos que ponham em causa as operações de negócio ou comprometam a segurança da informação são tratados como incidentes de segurança.

O processo de resposta a incidentes de segurança da informação e de cibersegurança do OMIP encontra-se sistematizado no seu Procedimento de Gestão de Incidentes, no qual se encontram definidas as tarefas de deteção, identificação, classificação, resposta, tratamento, comunicação, registo e reporte que devem ser realizadas após a deteção de um qualquer incidente de segurança da informação. Desta forma, o OMIP visa garantir uma resposta rápida e eficaz que permita minimizar os danos potenciais no negócio ao nível da confidencialidade, integridade e disponibilidade dos sistemas de informação.

A disponibilidade da informação, nomeadamente em caso de incidentes disruptivos, será ainda assegurada pelos Planos de Continuidade do Negócio definidos no âmbito do Sistema de Gestão da Continuidade do Negócio (BCMS) do OMIP.

4.9. Controlo de Acessos

As identidades e credenciais de acesso às redes e sistemas de informação do OMIP são emitidas, geridas, verificadas, revistas, revogadas e auditadas segundo os princípios do menor privilégio, da funcionalidade mínima e da segregação de funções. Estes princípios aplicam-se transversalmente a acessos internos (colaboradores), externos (fornecedores ou clientes) e remotos (internos ou externos).

Os mecanismos de autenticação nas redes e sistemas de informação do OMIP são definidos e mantidos de acordo com as suas características, sendo utilizada tecnologia de gestão de autenticação via *web* e via serviços de diretório, para acesso à informação da empresa. Nesse sentido, encontram-se implementados mecanismos de autenticação como a utilização de senhas, *tokens* criptográficos, sistema *Single Sign-On* (no caso da rede interna) e *multi-factor authentication* de forma a permitir a manutenção da integridade e confidencialidade da informação.

4.10. Segurança dos Dados e das Comunicações

As redes e os sistemas de informação do OMIP devem proteger a segurança (confidencialidade, integridade e disponibilidade) dos dados armazenados, dos dados em circulação, dos dados em utilização e dos fluxos de transferência da informação. Para tal, o OMIP tem implementados controlos de:

- Acesso físico e lógico e gestão de autenticação;
- Cópias de segurança e reposição;
- Registo de eventos;
- Classificação, manuseamento e destruição da informação;
- Criptografia;
- Prevenção de exfiltração de informação ou dados (vulgo DLP);
- Desenvolvimento seguro e restrição na utilização de *software*;
- Prevenção e deteção de atividade maliciosa.

4.11. Deteção de Eventos de Segurança

O OMIP recorre a serviços externos especializados em cibersegurança para a gestão de eventos de redes (*logs*), para a identificação de ameaças cibernéticas e para a avaliação periódica de vulnerabilidades nos sistemas de informação, nomeadamente através de processos automáticos de deteção, identificação, catalogação e monitorização de atividade maliciosa. Os resultados e tratamento das vulnerabilidades identificadas são posteriormente incorporados no plano interno de acção do OMIP, de forma a serem alvo de análise no âmbito da gestão do risco.

4.12. Cópias de Segurança

O OMIP realiza cópias de segurança da informação armazenada nos seus sistemas de informação, guardando as mesmas numa localização alternativa, quando possível, e garantido a manutenção da confidencialidade da informação. O OMIP assegura ainda a integridade e disponibilidade das cópias de segurança, estabelecendo para isso procedimentos de restauro que garantem a reposição eficiente das cópias de segurança em caso de necessidade, dentro do objetivo de tempo de recuperação. Estes procedimentos são testados com regularidade, de forma a validar a adequação dos mesmos, bem como, precisamente, a integridade e disponibilidade das cópias realizadas.

4.13. Testes

No âmbito da gestão do risco, o OMIP realiza testes para avaliar a eficácia dos controlos implementados para mitigação dos riscos identificados:

- Aplica um plano de testes de segurança para assegurar a manutenção da integridade, disponibilidade e confidencialidade da informação sempre que a sua infraestrutura sofre atualizações, seja por via da integração de um novo sistema de informação ou por alteração significativa de um sistema já existente;
- Recorre a serviços externos especializados para avaliação periódica de vulnerabilidades e realização de testes de intrusão à sua infraestrutura, cujos resultados e vulnerabilidades identificadas são posteriormente incorporados no plano interno de ação do OMIP, de forma a serem alvo de análise no âmbito da gestão do risco;
- Realiza testes periódicos aos seus procedimentos de gestão de incidentes e aos seus planos de continuidade de negócio (definidos no âmbito do Sistema de Gestão de Continuidade do

Negócio – BCMS), baseados em cenários plausíveis, com o objetivo de avaliar a sua eficácia e identificar pontos de falha e potenciais melhorias.

4.14. Cooperação e Partilha de Informação

A partilha de informação relevante em matéria de cibersegurança, não só com as partes interessadas, mas com outros grupos de interesse, associações ou organizações da indústria, permite alcançar uma consciência mais abrangente sobre cibersegurança.

A existência do Comité de Cibersegurança, a contratação de serviços externos especializados para a gestão de eventos de redes (*logs*) e para identificação de ameaças cibernéticas, bem como o protocolo de cooperação com o Centro Nacional de Cibersegurança, são alguns dos exemplos do compromisso do OMIP em contribuir para a concretização desse objetivo. Com estas partes são partilhados, através de canais seguros e em tempo útil, indicadores de compromisso, boas práticas, indicadores de risco e ainda experiências sobre ameaças, vulnerabilidades e ciberataques.

4.15. Melhoria Contínua

O OMIP está ciente não só da sua realidade dinâmica – ao nível dos processos de negócio, ativos e recursos humanos – mas também da constante evolução das ameaças de segurança e exploração de novas vulnerabilidades. Além disso, a segurança da informação e a cibersegurança são transversais a todas as atividades da organização, pelo que a sua melhoria contínua constitui um dos objetivos do OMIP.

Neste sentido, o OMIP atualiza os seus procedimentos, políticas, planos e processos à luz da atualização das boas práticas da indústria e das referências e normas internacionais de cibersegurança. Para além disso, tal revisão incorpora as oportunidades de melhoria propostas em auditorias, testes de intrusão, revisões da gestão ou outros projetos internos ou externos em matéria de segurança e cibersegurança, bem como as lições aprendidas no decorrer da resposta e recuperação de incidentes de segurança da informação.

5. Funções e responsabilidades

5.1. Conselho de Administração

O Conselho de Administração do OMIP detém, nos termos da regulamentação aplicável, a responsabilidade pela estratégia de resiliência operacional da Sociedade, onde se inclui, *inter alia*, a definição dos objetivos de segurança da informação e de cibersegurança, a definição e acompanhamento do perfil de risco do OMIP e a aprovação de um orçamento adequado para a implementação das práticas de segurança.

Ao Conselho de Administração, enquanto responsável máximo pela segurança da informação e cibersegurança, cabe a definição e aprovação da presente Política e de todos os documentos que a concretizem, bem como da sua revisão, de forma a garantir a sua contínua adequação e eficácia.

O Conselho de Administração deve ser mantido informado e deve acompanhar os desenvolvimentos e melhorias no ISMS, bem como os resultados de auditorias, testes e avaliações (internas ou externas) e desenvolvimentos que tenham sido objeto de deliberação expressa pelo Conselho de Administração.

5.2. 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 medidas de implementação e manutenção do ISMS, incluindo as estratégias de cibersegurança estabelecidas pelo Conselho de Administração, assegurando os recursos adequados para garantir a concretização dos objetivos definidos na presente Política e a conformidade da atividade prosseguida pela Sociedade.

5.3. Comité de Cibersegurança

O Comité de Cibersegurança do OMIE, OMIP SMGR e OMIClear é um comité interno de caráter técnico, criado a nível do Grupo OMI, composto pelas pessoas indicadas no Regulamento de Funcionamento do Comité de Cibersegurança do OMIE, OMIP SMGR e OMIClear. Conforme se mostre necessário, podem ser convidados a participar nas reuniões deste Comité outros colaboradores, nomeadamente os responsáveis pelo risco, os responsáveis dos departamentos jurídicos, os responsáveis pelo cumprimento e os auditores internos das sociedades.

O Comité de Cibersegurança é responsável por propor aos Conselhos de Administração das empresas que compõem o Grupo OMI estratégias e diretrizes no âmbito da cibersegurança, promovendo sinergias na implementação, cumprimento e monitorização dessas estratégias e requisitos nas diversas empresas e nos diferentes domínios de Administração, Proteção, Vigilância e Resiliência, devendo manter, através dos Diretores de Operações, os membros executivos dos Conselhos de Administração das diversas empresas informados de todos os assuntos relevantes em matéria de cibersegurança.

5.4. Comité de Segurança da Informação

No âmbito da implementação do Sistema de Gestão de Segurança da Informação (ISMS) no OMIP, foi constituído o Comité de Segurança da Informação do OMIP, sendo este um comité interno de caráter técnico e de apoio à gestão e decisão, composto, pelo menos, pelo Diretor de Operações, por um representante do departamento de Sistemas de Informação e pelo Gestor de Segurança da Informação do OMIP.

Conforme se mostre necessário, podem ser convidados a participar nas reuniões deste Comité outros colaboradores do OMIP, nomeadamente o responsável pelo departamento Jurídico ou outros colaboradores do departamento de sistemas de informação.

O Comité de Segurança é responsável pelo acompanhamento da implementação prática e manutenção das políticas e procedimentos do ISMS, bem como pela proposta de revisão das mesmas, a apresentar ao Conselho de Administração, de acordo com os objetivos e princípios que se encontram definidos na presente Política.

5.5. Gestor de Segurança da Informação

No âmbito da implementação do ISMS, o Conselho de Administração do OMIP designou um Gestor de Segurança da Informação que tem, como principais responsabilidades:

a) Promover programas de formação e sensibilização para a segurança da informação e cibersegurança junto de todos colaboradores, assegurando que a atuação dos mesmos se encontra em conformidade com todos os requisitos, políticas e procedimentos do ISMS;
b) Garantir que as não-conformidades do ISMS são corrigidas no mais curto espaço de tempo possível;

c) Garantir que o ISMS está de acordo com os seus objetivos, requisitos da ISO 27001 e demais requisitos regulamentares decorrentes da atividade do OMIP;
d) Ser o elo entre Comité de Segurança da Informação e as áreas e departamentos no âmbito do ISMS;
e) Levantar, no âmbito do Comité de Segurança da Informação do OMIP, a necessidade de proceder à revisão de Políticas e Procedimentos existentes em matéria de segurança da informação e cibersegurança;
f) Gerir e supervisionar o risco associado à segurança da informação e à cibersegurança;
g) Gerir e acompanhar as medidas adotadas pelo Conselho de Administração do OMIP em matéria de segurança da informação e cibersegurança;
h) Garantir a notificação dos incidentes TIC às Autoridades Competentes, nos termos da legislação aplicável.

O Gestor de Segurança da Informação participa no Comité de Segurança da Informação do OMIP e reporta diretamente ao Diretor de Operações e, sempre que necessário, ao Conselho de Administração.

5.6. Colaboradores

Os colaboradores do OMIP, nos quais, para os efeitos prosseguidos pela presente Política, se incluem os membros dos órgãos sociais do OMIP, devem compreender claramente os riscos de segurança da informação e de cibersegurança a que estão expostos no exercício das suas funções, bem como os seus papéis e responsabilidades no âmbito da mitigação desses riscos e da consequente proteção dos ativos do OMIP.

Em particular, os colaboradores do OMIP são responsáveis por:

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

5.7. Fornecedores

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

Os fornecedores são também responsáveis por reportar ao OMIP a ocorrência de incidentes de segurança da informação nos sistemas de informação do OMIP ou nos seus sistemas, na medida em que estes possam comprometer a cibersegurança do OMIP.

Os fornecedores cujo serviço prestado sustente uma função crítica ou importante do OMIP devem ser objeto de maior controlo, monitorização e requisitos de segurança da informação adicionais no âmbito da relação contratual entre as partes, conforme estabelecido na Política de Gestão de Fornecedores.

6. Disposições Finais

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

A presente Política encontra-se disponível para consulta no seu sítio institucional na *internet*.

Aprovado pelo Conselho de Administração a 26 de novembro de 2024