Política de Cibersegurança

28.mar.2023

Índice de Versões

16.dez.2020
Versão Inicial

22.nov.2022
Revisão geral

28.mar.2023
Inclusão da função OMIP de Administrador de Índices de Referência

Introdução

A Cibersegurança define-se 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 programas, plataformas ou outros serviços de informação.

O OMIP, enquanto 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), bem como Administrador de Índices de Referência, tal como definido no Regulamento (UE) 2016/1011 do Parlamento Europeu e do Conselho de 8 de junho de 2016 (RIR), tem a preocupação constante de estar dotado de um amplo conjunto de ferramentas de gestão da cibersegurança, de forma a garantir que os seus ativos e sistemas de informação estão em conformidade com os padrões, referências e normas internacionais, nomeadamente:

- ISO/IEC 27032:2012;
- ISO/IEC 27001:2013;
- Quadro Nacional de Referência para a Cibersegurança, Centro Nacional de Cibersegurança (CNCS);
- *Framework for Improving Critical Infrastructure Cybersecurity* (v1.1, April 16, 2018), NIST;

e ainda com os requisitos legais, nomeadamente com a 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) e com o 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.

Como mercado Regulamentado e nos termos do n.º 1 do artigo 29.º da Lei n.º 46/2018, o OMIP encontra-se identificado, pelo CNCS, como Operador de Serviço Essencial no sector das Infraestruturas do mercado financeiro (identificação atualizada anualmente pelo CNCS).

Atentos estes fatores, o OMIP estabelece, através da presente Política de Cibersegurança, os princípios da sua organização na gestão da cibersegurança, visando atingir os seguintes macro objetivos: Identificação, Proteção, Deteção, Resposta, Recuperação, Testes, Cooperação e partilha de informação e Melhoria contínua.

1. Âmbito

A presente Política aplica-se aos colaboradores, estagiários, prestadores de serviços e outros parceiros do OMIP, bem como a todos os seus ativos tecnológicos em operação, inativos ou em desenvolvimento.

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

2. Objetivos

São prosseguidos os seguintes objetivos para assegurar a Cibersegurança no OMIP:

a) Identificação
   i. Assegurar a conformidade com a legislação, regulamentação e demais normas aplicáveis;

ii. Cumprir com os requisitos de confidencialidade, integridade e disponibilidade adequados aos objetivos de negócio do OMIP, em particular com as necessidades dos seus membros e as determinações legais e regulamentares;
iii. Identificar e classificar os ativos de informação em função da sua relevância e criticidade, de forma a que possam ser adequadamente protegidos em todo o seu ciclo de vida;
iv. Assegurar que os fornecedores, nomeadamente os fornecedores que sejam considerados críticos pelo OMIP, se enquadram nas necessidades e requisitos de Cibersegurança;
v. Identificar, avaliar e tratar os riscos de Cibersegurança inerentes à atividade do OMIP e aos quais os seus ativos se encontram expostos;
vi. Estabelecer um procedimento de identificação, avaliação e tratamento do risco de acordo com a tolerância ao risco da organização;
vii. Implementar controlos e mecanismos de segurança que visam evitar, mitigar ou limitar os potenciais danos provocados pela exploração das vulnerabilidades dos ativos, de forma a minimizar 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.

b) Proteção
   i. Estabelecer e implementar controlos para proteger os ativos de informação do OMIP de roubo, intrusão, abuso ou outras formas de tratamento ilícito;
   ii. Assegurar a disponibilidade e fiabilidade dos equipamentos, infraestruturas e sistemas que suportam a atividade do OMIP;
   iii. Promover uma cultura de sensibilização e compromisso 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, de forma a minimizar o risco de incidentes de segurança da informação;
   iv. Assegurar a proteção de dados pessoais, nos termos previstos na legislação aplicável.

c) Deteção
   i. Monitorizar anomalias e eventos de cibersegurança, em tempo útil, e compreender o impacto potencial desses eventos;
   ii. Monitorizar continuamente as redes e sistemas de informação para identificar eventos de cibersegurança e verificar a eficácia das medidas de proteção aplicadas;
   iii. Implementar e manter processos de deteção de eventos anómalos.

d) Resposta
   i. Identificar, conter e solucionar incidentes de segurança da informação e, em particular, ciberataques;
   ii. Reduzir os danos no negócio inerentes à ocorrência de incidentes de segurança da informação, bem como minimizar o seu impacto para as partes interessadas do OMIP (internas e externas);
   iii. Garantir que os incidentes de segurança da informação são reportados em conformidade com a legislação em vigor e com os procedimentos internos definidos para o efeito.

e) Recuperação
    i. Assegurar que o OMIP tem a capacidade de prosseguir a prestação dos seus serviços, nomeadamente das suas funções de negócio críticas, caso ocorram incidentes de segurança da informação graves ou ciberataques, nas condições definidas na regulamentação, normas e procedimentos específicos aplicáveis;
    ii. Assegurar a redundância de equipamentos, infraestruturas e sistemas de informação que suportam as funções de negócio críticas, evitando assim pontos únicos de falha (vulgo SPOFs);
    iii. Minimizar os impactos negativos que possam advir da ocorrência de incidentes de segurança graves, tanto para a reputação da organização como para todas as partes interessadas do OMIP.

f) Testes
    i. Avaliar a eficácia dos controlos implementados no OMIP para mitigação dos riscos identificados;
    ii. Garantir a manutenção da integridade, disponibilidade e confidencialidade dos sistemas de informação do OMIP;
    iii. Identificar e mitigar as vulnerabilidades existentes na infraestrutura do OMIP;
    iv. Avaliar a eficácia e identificar pontos de falha e potenciais melhorias dos procedimentos e planos de resposta e recuperação a incidentes de segurança da informação.

g) Cooperação e partilha de informação
    i. 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;
    ii. Contribuir para a globalização da consciencialização sobre Cibersegurança.

h) Melhoria Contínua
    i. Atualizar os procedimentos, políticas, planos e processos do OMIP à luz da atualização das boas práticas da indústria e das referências e normas internacionais de Cibersegurança;
    ii. Promover estratégias de implementação de oportunidades de melhoria, nomeadamente as propostas resultantes de auditorias, testes de intrusão ou outros projetos internos ou externos em matéria de Cibersegurança;
    iii. Definir indicadores que suportem modelos de reporte de Cibersegurança a ser apresentados internamente ao Comité de Cibersegurança e, quando aplicável, a outros órgãos da empresa.

3. Funções e responsabilidades

3.1 Conselho de Administração

O Conselho de Administração do OMIP detém, em última instância, a responsabilidade global pela Cibersegurança e, em particular, pela definição da presente Política, bem como da sua revisão, de forma a garantir a sua contínua adequação e eficácia.

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 medidas de implementação e manutenção de estratégias de Cibersegurança, assegurando os recursos adequados para garantir a concretização dos objetivos definidos na presente Política.

3.3 Comité de Cibersegurança

O Comité de Cibersegurança do Grupo OMI é um comité interno de carácter técnico composto, pelo menos, pelos Diretores de Operações das empresas OMIP e OMIClear e pelo Diretor de Sistemas de Informação do OMIE.

O Comité de Cibersegurança é responsável por definir 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.

O Comité de Cibersegurança deverá manter o Presidente e o Vice-presidente e, se for o caso, os restantes membros dos respetivos Conselhos de Administração, informados de todos os assuntos relevantes em matéria de Cibersegurança.

3.4 Comité de Segurança

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

3.4 Colaboradores

Os colaboradores do OMIP devem compreender claramente os riscos 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, códigos, políticas e procedimentos definidos no âmbito da cibersegurança;
- Os activos de informação que lhe são confiados, devendo contribuir proactivamente para a devida protecção dos mesmos;
- Reportar a ocorrência de incidentes de segurança da informação no OMIP, nomeadamente de cibersegurança, de acordo com os procedimentos internos definidos para o efeito

3.5 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 sua

responsabilidade 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 ou em sistemas de informação do OMIP.

Os fornecedores que sejam consideradas críticos para o OMIP devem ser objeto de especiais exigências de controlo, monitorização e requisitos de segurança da informação adicionais no âmbito da relação contratual entre as partes.

4. Objetivos de Cibersegurança no OMIP

4.1 Identificação

4.1.1 Gestão de Ativos

A informação gerida pelo OMIP, os seus processos e infraestruturas de suporte, colaboradores, terceiras partes, equipamentos, documentos, sistemas, aplicações e redes são ativos relevantes para a organização. São, por isso, devidamente identificados, inventariados e classificados em função dessa mesma importância e criticidade, de forma a que possam ser adequadamente protegidos em todo o seu ciclo de vida (o qual inclui a sua criação, manuseamento, armazenamento, transporte e destruição).

4.1.2 Gestão de fornecedores

Na gestão de fornecedores, em particular os fornecedores que sejam considerados críticos, 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.

Na contratação de fornecedores é seguido um processo padrão, o qual inclui uma pesquisa de mercado a várias entidades às quais se reconheça competência e conhecimentos técnicos adequados para a prestação dos serviços ou fornecimento dos produtos.

4.1.3 Gestão do Risco

Uma das áreas fulcrais da Segurança da Informação e Continuidade de Negócio no OMIP é a gestão – identificação, análise, avaliação e tratamento – contínua dos riscos de segurança da informação, 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 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 da ocorrência de incidentes de segurança da informação e garantir um nível de segurança adequado face ao risco que o OMIP pode 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.

A gestão do risco do OMIP incorpora ainda o acompanhamento dos riscos operacionais aos quais o OMIP se encontra exposto, através do estabelecimento de procedimentos de avaliação do nível de exposição e do limite de risco considerado aceitável visando os objetivos da organização, de acordo com a Política de Risco Operacional.

4.2 Proteção

4.2.1 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 (de colaboradores), externos (de 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.

4.2.2 Segurança de 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 (vulgo DLP);
- Desenvolvimento seguro e restrição na utilização de *software*;
- Prevenção e deteção de atividade maliciosa.

4.2.3 Recursos Humanos

O OMIP promove ações de formação e sensibilização em Segurança da Informação e transmite a informação necessária para que a gestão de topo e os seus colaboradores estejam aptos a assumir as suas responsabilidades no âmbito da Cibersegurança. 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 Cibersegurança do OMIP têm ainda formação especializada na área de Segurança da Informação.

4.3 Deteção

O OMIP e as demais empresas do Grupo OMI recorrem a serviços externos especializados em Cibersegurança para a gestão de eventos de redes (*logs*) e para a avaliação periódica de vulnerabilidades sistemas de informação, nomeadamente através de processos automáticos de detecção, identificação, catalogação e monitorização de actividade 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.

4.4 Resposta

O processo de resposta a incidentes do OMIP encontra-se sistematizado em procedimentos de gestão de incidentes e, em particular, de ciberataques, nos quais se encontram definidas as tarefas de identificação, classificação, intervenção técnica, registo, tratamento e reporte que devem ser realizadas após a deteção de um incidente. 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.

Estes procedimentos, a par com outros procedimentos de comunicação e reporte transversais a todas as áreas da organização, definem ainda o plano de comunicações para as partes interessadas (internas e externas) do OMIP, com a finalidade de identificar, conter e solucionar o incidente, bem como de minimizar o seu impacto para essas mesmas partes interessadas.

4.5 Recuperação

4.5.1 Cópias de Segurança

O OMIP realiza cópias de segurança da informação crítica armazenada nos seus sistemas de informação, guardando as mesmas numa localização alternativa, quando possível, e garantindo 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.

4.5.2 Plano de Continuidade de Negócio e Planos de Recuperação da Atividade

A disponibilidade da informação, dos sistemas e da infraestrutura encontram-se asseguradas pela implementação de procedimentos de gestão e planos de recuperação de incidentes de segurança da informação graves ou ciberataques com impactos disruptivos. Deste modo e na ocorrência de tais incidentes, o OMIP tem a capacidade de prosseguir a prestação dos seus serviços, nomeadamente das suas funções de negócio críticas, em condições adequadas e nos termos definidos na regulamentação, normas e procedimentos específicos aplicáveis, minimizando assim os impactos negativos que daí possam advir, tanto para a reputação da organização como para todas as partes interessadas do OMIP.

No que diz respeito à redundância da infraestrutura, o centro de processamento de dados (*Datacenter*) secundário do OMIP encontra-se numa localização distinta (com um perfil de risco geográfico distinto) e é sincronizado, em tempo real, com o *Datacenter* principal, de forma a minimizar o tempo de disrupção da operação do OMIP.

4.6 Testes

No âmbito da gestão do risco, o OMIP realiza testes para avaliar a eficácia dos controlos implementados para mitigação dos riscos identificados. Além disso, sempre que a infraestrutura do OMIP sofre atualizações, seja por via da integração de um novo sistema de informação ou por alteração significativa de um sistema já existente, é aplicado um plano de testes de segurança para assegurar a manutenção da integridade, disponibilidade e confidencialidade da informação.

O OMIP realiza ainda testes periódicos aos seus procedimentos de gestão de incidentes e de ciberataques e aos planos de continuidade de negócio e de recuperação de *Datacenter*, baseados em cenários plausíveis, com o objetivo de avaliar a sua eficácia e identificar pontos de falha e potenciais melhorias.

4.7 Cooperação e partilha de informação

A informação relevante em matéria de Cibersegurança é partilhada com as partes interessadas do OMIP, bem como com o Comité de Cibersegurança do Grupo OMI. Por outro lado, o OMIP coopera com o Centro Nacional de Cibersegurança, com base num protocolo de cooperação partilhando, através de canais seguros e em tempo útil, indicadores de compromisso, boas práticas, indicadores de risco e ainda experiências sobre ameaças, vulnerabilidades e ciberataques

Adicionalmente, o OMIP colabora com outros grupos de interesse, associações ou organizações da indústria, de forma a alcançar uma consciência mais abrangente sobre Cibersegurança.

4.8 Melhoria Contínua

O OMIP está ciente não só da sua realidade dinâmica – ao nível dos processos de negócio, activos e recursos humanos – mas também da constante evolução das ciberameaças e exploração de novas vulnerabilidades. Ademais, a Cibersegurança é transversal a todas as actividades 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 por auditorias, testes de intrusão ou outros projetos internos ou externos em matéria de Cibersegurança, bem como as lições aprendidas no decorrer da resposta e recuperação de incidentes de segurança da informação.

Como medida de monitorização desta melhoria contínua, o OMIP tem acesso a um conjunto de dados/indicadores que poderão ser utilizados para apresentação interna ao Comité de Segurança, Comité de Cibersegurança e, quando aplicável, a outros órgãos da empresa.

5. Disposições Finais

A presente Política deve ser revista pelo Conselho de Administração sempre que se verifique alguma alteração no âmbito da Cibersegurança, 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 a 28 de março de 2023