omiclear

Política de Ciberseguridad

30.nov.2022

Índice de versiones

31.mar.2020
Versión inicial

30.nov.2022
Revisión general

CLÁUSULA DE EXENCIÓN DE RESPONSABILIDAD

El siguiente texto en lengua española no es una traducción oficial y su único propósito es informar. El documento original está escrito en lengua portuguesa (disponible en www.omiclear.eu). Si hubiera alguna discrepancia entre el original portugués y la traducción española, prevalecerá el original portugués. Aunque se han realizado todos los esfuerzos para proporcionar una traducción exacta, no nos hacemos responsables de la exactitud de la traducción y no será asumida ninguna responsabilidad por el uso o la confianza depositada en la traducción española, ni por los errores o malos entendidos que de ella se puedan derivar.

Este documento está disponible en www.omiclear.eu

Introducción

La ciberseguridad se define como la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, es decir, en el espacio no físico creado por redes de ordenadores, concretamente por Internet, donde las personas se pueden comunicar e interactuar por medio de programas, plataformas u otros servicios de información.

OMIClear, como Contraparte Central (CCP) autorizada en los términos del EMIR, tiene la preocupación constante de estar dotada de un amplio conjunto de herramientas de gestión de ciberseguridad, de forma a garantizar que sus activos y sistemas de información están en conformidad con los estándares, referencias y normas internacionales, específicamente:

- 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, 16 de abril de 2018), NIST;
- *Cyber resilience oversight expectations for financial market infrastructures* (Diciembre 2018), Banco Central Europeo;

así como con los requisitos legales, concretamente con la ley n.º 46/2018 (de 13 de agosto) que establece el régimen jurídico de la seguridad del ciberespacio (trasponiendo la Directiva (UE) n.º 2016/1148, del Parlamento Europeo y del Consejo de 6 de julio de 2016) y con el Decreto-ley 65/2021, de 30 de julio, por el que se regula el régimen jurídico de la seguridad en el ciberespacio y se definen las obligaciones de certificación en materia de ciberseguridad en aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo, de 17 de abril de 2019.

En concreto, como CCP y en virtud de los términos del artículo 29.1 de la Ley n.º 46/2018, OMIClear está identificada por el CNCS, como Operador de Servicio Esencial en el sector de las Infraestructuras del mercado financiero (identificación actualizada anualmente por el CNCS).

Atenta a estos factores, OMIClear establece, a través de la presente Política de ciberseguridad, los principios de su organización en la gestión de la ciberseguridad, con el objetivo de alcanzar los siguientes macroobjetivos: identificación, protección, detección, respuesta, recuperación, pruebas, cooperación e intercambio de información y mejora continua.

1. Ámbito

La presente Política se aplica a los empleados, becarios, prestadores de servicios y otros socios de OMIClear, así como a todos sus activos tecnológicos en operación, inactivos o en desarrollo.

El ámbito de aplicación de esta Política se extiende a todas las áreas de funcionamiento de OMIClear cuya actuación tiene impactos en ciberseguridad.

2. Objetivos

Se persiguen los siguientes objetivos para garantizar la ciberseguridad en OMIClear:

a) Identificación
   i. Asegurar la conformidad con la legislación, regulación y demás normas aplicables;
   ii. Cumplir con los requisitos de confidencialidad, integridad y disponibilidad adecuados a los objetivos de negocio de OMIClear, en particular con las necesidades de sus miembros;

iii. Identificar y clasificar los activos de información en función de su relevancia y criticidad de forma que se puedan clasificar adecuadamente en todo su ciclo de vida;
iv. Asegurar que los proveedores, a saber, los proveedores considerados críticos por OMIClear, se enmarcan en las necesidades y requisitos de ciberseguridad;
v. Identificar, evaluar y tratar los riesgos de ciberseguridad inherentes a la actividad de OMIClear y a los que sus activos se encuentran expuestos;
vi. Establecer un procedimiento de identificación, evaluación y tratamiento del riesgo de acuerdo con la tolerancia al riesgo de la organización;
vii. Implementar controles y mecanismos de seguridad cuyo objetivo sea evitar, mitigar o limitar los potenciales daños provocados por la exploración de las vulnerabilidades de los activos, de forma a minimizar la ocurrencia de incidentes de seguridad de la información y garantizar un nivel de seguridad adecuado de cara al riesgo que OMIClear está dispuesta a asumir.

b) Protección
   i. Establecer e implementar controles para proteger los activos de información de OMIClear de robo, intrusión, abuso u otras formas de tratamiento ilícito;
   ii. Garantizar la disponibilidad y fiabilidad de los equipamientos, infraestructuras y sistemas que soportan la actividad de OMIClear;
   iii. Promover una cultura de sensibilización y compromiso para la ciberseguridad entre los miembros del Consejo de Administración, la alta dirección y los empleados, motivándolos a que tomen conocimiento y asuman la responsabilidad de su intervención, de forma a minimizar el riesgo de incidentes de seguridad de la información;
   iv. Garantizar la protección de datos personales, en los términos previstos en la legislación aplicable.
c) Detección
   i. Monitorizar anomalías y eventos de ciberseguridad, en tiempo útil, y comprender el impacto potencial de esos eventos;
   ii. Monitorizar continuamente las redes y sistemas de información para identificar eventos de ciberseguridad y comprobar la eficacia de las medidas de protección aplicadas;
   iii. Implementar y mantener procesos de detección de eventos anómalos.
d) Respuesta
   i. Identificar, contener y solucionar incidentes de seguridad de la información y, en particular, ciberataques;
   ii. Reducir los daños al negocio inherentes a la ocurrencia de incidentes de seguridad de la información, así como minimizar su impacto para las partes interesadas de OMIClear (internas y externas);
   iii. Garantizar que los incidentes de seguridad de la información son reportados de conformidad con la legislación vigente y con los procedimientos internos definidos al efecto.
e) Recuperación
   i. Asegurar que OMIClear tiene la capacidad de continuar prestando sus servicios, concretamente sus funciones de negocio críticas, si ocurren incidentes de seguridad de la información graves o ciberataques, en las condiciones definidas en el reglamento, las normas y procedimientos específicos aplicables;

   ii. Garantizar la redundancia de equipamientos, infraestructuras y sistemas de información que soportan las funciones de negocio críticas, evitando así puntos únicos de fallo (conocidos como SPOF);
   iii. Minimizar los impactos negativos que pueden derivarse de la ocurrencia de incidentes de seguridad graves, tanto para la reputación de la organización como para todas las partes interesadas de OMIClear.

f) Pruebas
   i. Evaluar la eficacia de los controles aplicados en OMIClear para mitigar los riesgos identificados;
   ii. Garantizar el mantenimiento de la integridad, disponibilidad y confidencialidad de los sistemas de información de OMIClear;
   iii. Identificar y mitigar las vulnerabilidades existentes en la infraestructura de OMIClear;
   iv. Evaluar la eficacia e identificar puntos de fallo y potenciales mejoras de los procedimientos y planes de respuesta y recuperación a incidentes de seguridad de la información.

g) Cooperación e intercambio de información
   i. Fomentar el intercambio de información relevante en materia de ciberseguridad, a través de canales seguros y en tiempo útil, con las partes interesadas de OMIClear y otros grupos de interés;
   ii. Contribuir a la globalización de la concienciación sobre ciberseguridad

h) Mejora continua
   i. Actualizar los procedimientos, políticas, planes y procesos de OMIClear a raíz de la actualización de las buenas prácticas del sector y de las referencias y normas internacionales de ciberseguridad;
   ii. Fomentar estrategias de implementación de oportunidades de mejora, concretamente las propuestas resultantes de auditorías, pruebas de intrusión u otros proyectos internos o externos en materia de ciberseguridad;
   iii. Definir indicadores que apoyen modelos de informe de ciberseguridad que se presentarán internamente al Comité de Ciberseguridad y, cuando corresponda, a otros órganos de la empresa.

3. Funciones y responsabilidades

3.1 Consejo de administración

El Consejo de Administración de OMIClear ostenta, en última instancia, la responsabilidad global sobre ciberseguridad y, en particular, de la definición de la presente Política, así como de su revisión, de forma a garantizar su continua adecuación y eficacia.

3.2 Alta dirección

La Alta dirección de OMIClear, constituida por el Presidente y el Vicepresidente del Consejo de Administración y del Director de Operaciones, ostenta la responsabilidad de apoyar y soportar todas las medidas de implementación y mantenimiento de estrategias de ciberseguridad, asegurando los recursos adecuados para garantizar la concretización de los objetivos definidos en la presente Política.

3.3 Comité de Ciberseguridad

El Comité de Ciberseguridad del Grupo OMI es un comité interno de carácter técnico formado, al menos, por los Directores de Operaciones de las empresas OMIClear y OMIP y por el Director de Sistemas de Información de OMIE.

El Comité de Ciberseguridad es responsable de la definición de estrategias y directrices en el marco de la ciberseguridad, fomentando sinergias en la implementación, cumplimiento y monitorización de dichas estrategias y requisitos en las diversas empresas y en los diferentes dominios de Administración, Protección, Vigilancia y Resiliencia.

El Comité de Ciberseguridad deberá mantener al Presidente y al Vicepresidente y, si corresponde, a los restantes miembros de los respectivos Consejos de Administración, informados de todos los asuntos relevantes en materia de ciberseguridad.

3.4 Comité de Seguridad

En el contexto de la implantación del Sistema de Gestión de Seguridad de la Información (ISMS), se ha creado el Comité de Seguridad de OMIClear, que es un comité interno de carácter técnico, compuesto, como mínimo, por el Director de Operaciones, un representante del Departamento de Sistemas de Información y el Responsable de Seguridad de la Información. El Comité de Seguridad también es responsable de la aplicación, mantenimiento y revisión de las políticas y procedimientos de ciberseguridad, de acuerdo con los objetivos y principios definidos en esta Política.

3.5 Empleados

Los empleados de OMIClear deben comprender claramente los riesgos de ciberseguridad a los que están expuestos en el ejercicio de sus funciones, así como sus papeles y responsabilidades en el marco de la mitigación de esos riesgos y de la consiguiente protección de los activos de OMIClear.

En particular, los empleados de OMIClear son responsables de:

- Cumplir todas las normas, códigos, políticas y procedimientos definidos en el ámbito de la ciberseguridad;
- Los activos de información que se les confían, debiendo contribuir proactivamente a la debida protección de los mismos;
- Notificar la ocurrencia de incidentes de seguridad de la información en OMIClear, concretamente incidentes de ciberseguridad, de conformidad con los procedimientos internos definidos a tal efecto.

3.6 Proveedores

Los proveedores deben adoptar conductas y procedimientos consistentes con la presente política. En particular, los contratos entre OMIClear y las empresas prestadoras de servicios con acceso a sus sistemas de información y/o entorno tecnológico deben contener cláusulas y requisitos de seguridad que garanticen la confidencialidad entre las partes y que aseguren que los profesionales bajo su responsabilidad cumplan la presente Política, norma, códigos y demás procedimientos que sean aplicables.

Los proveedores son también responsables de informar a OMIClear sobre la ocurrencia de incidentes de seguridad de la información o en sistemas de información de OMIClear.

Los proveedores y otras entidades externas que se consideren críticas para OMIClear deberán ser objeto de un mayor control, supervisión y requisitos adicionales de seguridad de la información, en el contexto de la relación contractual entre las partes.

4. Objetivos de ciberseguridad en OMIClear

4.1 Identificación

4.1.1 Gestión de activos

La información gestionada por OMIClear, sus procesos e infraestructuras de apoyo, empleados, terceras partes, equipamientos, documentos, sistemas, aplicaciones y redes son activos relevantes para la organización. Son, por ello, debidamente identificados, inventariados y clasificados en función de esa misma importancia y criticidad, de forma que pueden ser adecuadamente protegidos en todo su ciclo de vida (que incluye su creación, manipulación, transporte y destrucción).

4.1.2 Gestión de proveedores y prestadores de servicios

En la gestión de proveedores, en particular de los considerados críticos, OMIClear sigue los principios establecidos en su Política de Gestión de Proveedores, a saber, la definición de requisitos de seguridad de la información para la mitigación de los riesgos asociados al acceso de los proveedores (y de la cadena de suministro de tecnologías de la información y de la comunicación) a los activos de información, así como el mantenimiento del nivel de seguridad de la información y de disponibilidad de los servicios prestados de acuerdo con las condiciones contratadas con los proveedores, mediante el establecimiento de procedimientos de seguimiento y evaluación de la prestación de servicios por parte de los proveedores.

A la hora de contratar proveedores, OMIClear sigue un proceso estándar, en el que hace un estudio de mercado a varias entidades a las que les reconozca competencia y conocimientos técnicos adecuados para la prestación o suministro de los productos o servicios en causa, siendo elaborado un pliego de condiciones específico con información completa sobre el objeto de la contratación, las condiciones de contratación y los criterios de adjudicación. Además, se pueden solicitar certificaciones y referencias para otorgar credibilidad y transparencia a cada propuesta.

4.1.3 Gestión del riesgo

Una de las áreas centrales de la Seguridad de la Información y Continuidad de Negocio en OMIClear es la gestión –identificación, evaluación y tratamiento– continua de los riesgos de seguridad de la información, inherentes a su actividad, a los que los se encuentran expuestos los activos de la organización, que constituye una herramienta de gestión de la empresa.

La metodología de gestión del riesgo de OMIClear implica:

- Identificación y documentación de las amenazas internas y externas que puedan explotar las vulnerabilidades de los activos de OMIClear, poniendo en entredicho la integridad, confidencialidad o disponibilidad de los mismos;
- evaluación basada en escenario de riesgo para el que se analizó la probabilidad y el impacto que componen el nivel de riesgo;
- tratamiento de los riesgos, de acuerdo con la criticidad del activo y los criterios de aceptación y priorización del riesgo de la organización.

En el ámbito del tratamiento, la gestión del riesgo incluye la implementación de controles y mecanismos de seguridad cuyo objetivo es reducir, transferir, evitar o aceptar los potenciales daños provocados por la explotación de las vulnerabilidades de los activos, de forma a minimizar la ocurrencia de incidentes de seguridad de la información y garantizar un nivel de seguridad adecuado en virtud del riesgo que OMIClear está dispuesta a asumir. Estas medidas se definen de acuerdo con los objetivos de negocio y las responsabilidades de OMIClear, teniendo en cuenta la eficiencia, el coste y su aplicabilidad.

La gestión del riesgo de OMIClear incorpora también el seguimiento de los riesgos operativos a los que OMIClear se encuentra expuesta, a través del establecimiento de procedimientos de evaluación del nivel de exposición y del límite de riesgo considerado aceptable con vistas a los objetivos de la organización, de acuerdo con la Política de Riesgo Operacional.

4.2 Protección

4.2.1 Control de accesos

Las identidades y credenciales de acceso a las redes y sistemas de información de OMIClear se emiten, gestionan, comprueban, revisan, revocan y auditan según los principios del menor privilegio, de la funcionalidad mínima y de la segregación de funciones. Estos principios se aplican transversalmente a accesos internos (de empleados), externos (de proveedores o clientes) y remotos (internos o externos).

Los mecanismos de autenticación en las redes y sistemas de información de OMIClear se definen y mantienen de acuerdo con sus características, utilizando tecnología de gestión de autenticación vía web y vía servicios de directorio, para el acceso a la información de la empresa. En este sentido, se implementan mecanismos de autenticación como el uso de contraseñas, tokens criptográficos, sistema Single Sign-On (en el caso de la red interna) y autenticación multifactor, para permitir el mantenimiento de la integridad y confidencialidad de la información.

4.2.2 Seguridad de datos y de las comunicaciones

Las redes y los sistemas de información de OMIClear deben proteger la seguridad (confidencialidad, integridad y disponibilidad) de los datos almacenados, de los datos en circulación, de los datos en utilización y de los flujos de transferencia de la información. Para ello, OMIClear ha implementado los controles de:

- Acceso físico y lógico y gestión de la autenticación;
- Copias de seguridad y reposición;
- Registro de eventos;
- Clasificación, manipulación y destrucción de la información;
- Criptografía;
- Prevención de exfiltración de información (conocido como DLP);
- Desarrollo seguro y restricción en el uso de s*oftware*;
- Prevención y detección de actividad maliciosa.

4.2.3 Recursos Humanos

OMIClear promueve acciones de formación y sensibilización en Seguridad de la Información y transmite la información necesaria para que la alta dirección y sus empleados sean aptos para asumir su responsabilidad en el ámbito de la ciberseguridad. OMIClear valida posteriormente el éxito y eficacia de estas acciones a través de campañas de, por ejemplo, simulación de eventos.

Los empleados de los departamentos con accesos privilegiados a las redes y los sistemas de información de OMIClear tienen, adicionalmente y antes de asumir funciones, formación específica sobre gestión de accesos y demás procedimientos operacionales. Los empleados con responsabilidades añadidas en Ciberseguridad de OMIClear tienen, además, formación especializada en el área de Seguridad de la Información.

4.3 Detección

OMIClear y las demás empresas del Grupo OMI recurren a servicios de un socio especialista en ciberseguridad, con lo que cuentan con un SOC (Centro de Operaciones de Seguridad) Externalizado. La principal función del SOC de OMIClear es la gestión y correlación de registros y eventos de redes y sistemas de información, que consiste en procesos de identificación, catalogación, monitorización y detección de actividad maliciosa.

4.4 Respuesta

El proceso de respuesta a incidentes de OMIClear está sistematizado en procedimientos de gestión de incidentes y, en particular, de ciberataques, en los que se encuentran definidas las tareas de identificación, clasificación, ejecución técnica, registro, tratamiento y reporte que deben ser realizadas después de detectar un incidente. De esta forma, OMIClear pretende garantizar una respuesta rápida y eficaz que permita minimizar los daños potenciales en el negocio a nivel de la confidencialidad, integridad y disponibilidad de los sistemas de información.

Estos procedimientos, junto con otros procedimientos de comunicación e informe transversales a todas las áreas de la organización, definen también el plan de comunicaciones para las partes interesadas (internas y externas) de OMIClear, con la finalidad de identificar, contener y solucionar el incidente, así como de minimizar su impacto para esas mismas partes interesadas.

4.5 Recuperación

4.5.1 Copias de seguridad

OMIClear realiza copias de seguridad de la información almacenada en sus sistemas de información, guardando las mismas en una localización alternativa, cuando sea posible, y garantizando el mantenimiento de la confidencialidad de la información. OMIClear asegura además la integridad y disponibilidad de las copias de seguridad, estableciendo para ello procedimientos de restauración que garanticen la reposición eficiente de las copias de seguridad en caso de necesidad dentro del objetivo de tiempo de recuperación. Estos procedimientos se prueban con regularidad, de forma a validar la adecuación de los mismos, así como, precisamente, la integridad y disponibilidad de las copias realizadas.

4.5.2 Plan de continuidad de negocio y Planes de recuperación de la actividad

La disponibilidad de la información, de los sistemas y de la infraestructura se encuentra asegurada por la aplicación de procesos de gestión y planes de recuperación de incidentes de seguridad de la información graves o ciberataques con impactos disruptivos. De este modo y ante la ocurrencia de tales incidentes, OMIClear tiene la capacidad de continuar prestando sus servicios, concretamente sus funciones de negocio críticas, en condiciones adecuadas y en los términos definidos en la regulación, normas y procedimientos específicos aplicables, minimizando así los impactos negativos que de allí

puedan derivar, tanto para la reputación de la organización como para todas las partes interesadas de OMIClear.

En lo referente a la redundancia de la infraestructura, el centro de procesamiento de datos (*Datacenter*) secundario de OMIClear se encuentra en una localización distinta (con un perfil de riesgo geográfico distinto) y es sincronizado, en tiempo real, con el *Datacenter* principal, de forma a minimizar el tiempo de disrupción de la operación de OMIClear.

4.6 Pruebas

En el marco de la gestión del riesgo, OMIClear realiza pruebas para evaluar la eficacia de los controles aplicados para la mitigación de los riesgos identificados. Además, siempre que la infraestructura de OMIClear sufre actualizaciones, tanto por vía de la integración de un nuevo sistema de información como debido a la alteración significativa de un sistema ya existente, se aplica un plan de pruebas de seguridad para garantizar el mantenimiento de la integridad, disponibilidad y confidencialidad de la información.

OMIClear recurre a servicios externos especializados para evaluar periódicamente vulnerabilidades y realizar pruebas de intrusión a su infraestructura, cuyos resultados y vulnerabilidades identificadas son posteriormente incorporados en el plan interno de acción de OMIClear, para que sean objeto de análisis en el marco de la gestión del riesgo.

OMIClear realiza además pruebas periódicas a sus procedimientos de gestión de incidentes y de ciberataques y a los planes de continuidad de negocio y de recuperación de *Datacenter*, basadas en escenarios posibles, con el objetivo de evaluar su eficacia e identificar puntos de fallo y potenciales mejoras.

4.7 Cooperación e intercambio de información

El intercambio de información relevante en materia de ciberseguridad, no solo con las partes interesadas de OMIClear, sino con otros grupos de interés, asociaciones u organizaciones del sector, permite alcanzar una consciencia más amplia sobre ciberseguridad.

El Comité de ciberseguridad y el SOC de OMIClear, así como el protocolo de cooperación con el Centro Nacional de Ciberseguridad, son algunos de los ejemplos del compromiso de OMIClear para contribuir a la realización de dicho objetivo. Con esas partes se intercambian, a través de canales seguros y en tiempo útil, indicadores de compromiso, buenas prácticas, indicadores de riesgo y experiencias sobre amenazas, vulnerabilidades y ciberataques.

4.8 Mejora continua

OMIClear es consciente no solo de su realidad dinámica –a nivel de los procesos de negocio activos y recursos humanos– sino también de la constante evolución de las ciber amenazas y explotación de nuevas vulnerabilidades. Además, la Ciberseguridad es transversal a todas las actividades de la organización, por lo que su mejora continua constituye uno de los objetivos de OMIClear.

En este sentido, OMIClear actualiza sus procedimientos, políticas, planes y procesos a la luz de la actualización de las buenas prácticas del sector y de las referencias y normas internacionales de ciberseguridad. Además, dicha revisión incorpora las oportunidades de mejora propuestas por auditorías, pruebas de intrusión u otros proyectos internos y externos en materia de ciberseguridad, así como las lecciones aprendidas en el transcurso de la respuesta y recuperación de incidentes de seguridad de la información.

Como medida de monitorización de dicha mejora continua, OMIClear ha definido un conjunto de indicadores que soportan modelos de informe de ciberseguridad, que se presentan internamente al Comité de ciberseguridad y, cuando se aplique, a otros órganos de la empresa.

5. Disposiciones finales

La presente Política debe ser revisada por el Consejo de Administración siempre que se verifique alguna modificación en el ámbito de la ciberseguridad, en la organización interna de OMIClear, en el marco legal y regulatorio o en las mejores prácticas seguidas por el sector.

La presente Política se encuentra disponible para consulta en su site corporativo.

Aprobado por el Consejo de Administración el 30 de noviembre de 2022