POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Documento de uso interno

Índice

CONTROL DE CAMBIOS

HISTÓRICO DE CAMBIOS		
VERSIÓN	**DESCRIPCIÓN DEL CAMBIO**	**FECHA DE APROBACIÓN**
1	Primera edición del documento	21/04/2021
2	Actualización RD 311 /2022 (nuevo ENS)	15/12/2023
3	Corrección alcance	14/01/2026

1. Aprobación y entrada en vigor

Texto aprobado el día 15 de diciembre de 2023 por la Dirección de **MUNDIAUDIT**.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha hasta que sea reemplazada por una nueva versión.

2. Introducción

MUNDIAUDIT depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada a los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuidad de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, y seguir los niveles de prestación de los servicios, seguir y analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

MUNDIAUDIT debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos TIC.

MUNDIAUDIT debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, en adelante (ENS).

3. Alcance

Esta Política de seguridad será de obligado cumplimiento para todos los miembros de **MUNDIAUDIT** que dan soporte a las actividades de prestación de los siguientes servicios:

- Auditoria contable, financiera y legal
- Consultoría de empresas
- Auditoria de sistemas
- Diseño, análisis, desarrollo y puesta en marcha y mantenimiento de software conforme con la declaración de aplicabilidad vigente.

4. Misión

MUNDIAUDIT es un referente en el ámbito de la consultoría y asesoría empresarial que se distingue por su solvencia, excelencia y calidad.

Fundada en 1999 para dar respuesta a la creciente demanda de transparencia en la gestión de empresas y sociedades, contamos en la actualidad con una gran cartera de clientes integrada por firmas e instituciones de diferentes sectores y tamaños, a escalas nacional e internacional, y con un equipo multidisciplinar de profesionales especializados

Nuestra metodología, basada en el uso de las más avanzadas herramientas y sistemas tecnológicos, nos permiten satisfacer la creciente demanda de nuestros servicios.

En **MUNDIAUDIT**:

- Minimizamos los tiempos de presencia en las sedes de nuestros clientes.
- Creamos equipo, establecemos una relación próxima.
- Potenciamos una comunicación permanente y fluida.
- Garantizamos la máxima discreción y confidencialidad.

MUNDIAUDIT busca el éxito de sus clientes, a través del compromiso, una atención personalizada y la máxima eficacia. Nuestra apuesta por la transparencia, el liderazgo, la exigencia, la perseverancia, la disciplina y la responsabilidad, señas de identidad de nuestra firma y de nuestros profesionales.

5. Marco normativo

Se toma como referencia básica en materia de Seguridad de la Información la normativa siguiente:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.
- Ley 34/2002, de 11 de junio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley de Propiedad Industrial

6. Principios básicos

6.1 Prevención

MUNDIAUDIT debe evitar, o al menos prevenir en la medida de lo posibles, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS y cualquier control adicional identificado mediante una evolución de amenazas y riesgos. Estos controles, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por terceros para obtener una evaluación independiente.

6.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

6.3 Respuesta

MUNDIAUDIT:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa puntos de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6.4 Conservación

Para garantizar la disponibilidad de los servicios críticos, las distintas áreas de **MUNDIAUDIT** deben conservar la información adecuadamente y desarrollar, cuando sea necesario, planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio de actividades de recuperación.

7. Organización de la seguridad

La implantación de la Política de Seguridad en **MUNDIAUDIT** requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información

b) Responsables del Servicio

c) Responsables de la Información

d) Responsable de Seguridad de la Información

e) Responsable de Sistemas

En estos apartados se especifican las funciones atribuidas a cada rol.

7.1 Comité de seguridad de la información

La seguridad de la Información es una responsabilidad organizativa que es compartida con la Dirección. Así, la Dirección de MUNDIAUDIT promueve la composición de un Comité de Seguridad de la Información, para establecer una vida definida y el apoyo a las iniciativas de seguridad.

Dicho Comité lo componen las figuras mencionadas.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales;

- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.

- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dichos activos;
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.

- Supervisión y seguimiento de aspectos tales como:

    - Principales incidencias en la Seguridad de la Información;
    - Elaboración y actualización de planes de continuidad
    - Cumplimiento y difusión de las Políticas de Seguridad

7.2 Responsable de la Información

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos

- Determina los niveles de seguridad de la información.

7.3 Responsable del Servicio

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad de la información.

7.4 Responsable de Seguridad de la Información

Responsable de la definición, coordinación, implantación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos de la Dirección General.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de **MUNDIAUDIT**.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
    - La estrategia de seguridad de la información definida por el Comité de Seguridad.
    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de **MUNDIAUDIT** y normativa de desarrollo.
- Supervisar (como responsable último) los incidentes de seguridad informática producidas en **MUNDIAUDIT**
- Difundir en **MUNDIAUDIT** las normas y procedimientos contenidos en la Política de Seguridad de la Información de **MUNDIAUDIT** y normativa de desarrollo, así como las funciones y obligaciones de todo **MUNDIAUDIT** en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables tales como el RGPD.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de **MUNDIAUDIT**.

7.5 Responsable del Sistema

Es responsable último de asegurar la ejecución de medidas para asegurar los activos y servicios de los Sistemas de Información, que soportan la actividad de **MUNDIAUDIT**, de acuerdo a los objetivos estratégicos de **MUNDIAUDIT**.

Las funciones del Responsable de Sistemas de la Información son las siguientes:

- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de **MUNDIAUDIT**, conforme a la estrategia de seguridad definida.
- Establecer la actuación de los Responsables Técnicos Informáticos, en los distintos entornos de seguridad que se designen.
- Garantizar la actualización del inventario de activos de Sistemas de Información de **MUNDIAUDIT**.
- Asegurar que existe el nivel de seguridad informática adecuado para cada uno de los activos inventariados, coordinando el correcto desarrollo, implantación, adecuación y operación de los controles y medidas destinados a garantizar el nivel de protección requerido.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en **MUNDIAUDIT**.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- Mantener y actualizar las directrices y políticas de seguridad de los Sistemas de Información y normativa asociada.

8. Procedimientos de designación

Se designan las siguientes responsabilidades:

- **Responsable del Servicio y de la Información**: Néstor García Estupiñán
- **Responsable de Seguridad**: Raúl J. Benavente Mejías
- **Responsable del Sistema**: Dailos Ramos Suárez

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

El Responsable de Seguridad de la Información será nombrado por la Dirección a propuesta del Comité de Seguridad.

8.1 Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa, éste será resuelto por el superior jerárquico de los mismos con la mediación del Responsable de Seguridad, elevándose para su resolución a la Dirección en caso de no llegar a un acuerdo.

En la resolución de estas controversias se tendrán en cuenta las exigencias derivadas de la protección de datos personales.

9. Revisión de la política de seguridad de la información

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

10. Datos de carácter personal

MUNDIAUDIT trata datos de carácter personal.

Todos los sistemas de información de **MUNDIAUDIT** se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado 5. Marco Normativo, de la presente Política de Seguridad de la Información.

11. Gestión de riesgos

Para todos los sistemas sujetos a esta Política de Seguridad de la Información se debe evaluar periódicamente los expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información gestionada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

12. Desarrollo de la política de seguridad de la información

Esta política de seguridad de la Información complementa las políticas de seguridad de **MUNDIAUDIT** en materia de protección de datos de carácter personal.

Esta Política de Seguridad de la Información se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

13. Obligaciones del personal

Todos y cada uno de los usuarios de los sistemas de información de **MUNDIAUDIT** son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros de **MUNDIAUDIT** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de **MUNDIAUDIT** recibirán formación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **MUNDIAUDIT**, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

13.1 Incumplimiento

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

14. Terceras partes

Las empresas y organizaciones externas que con ocasión de su colaboración con **MUNDIAUDIT** para la prestación de un servicio, accedan o gestionen activos de información de **MUNDIAUDIT** o de sus usuarios, directa o indirectamente (en sistemas propios o ajenos), comparten la responsabilidad de mantener la seguridad de los sistemas y activos del **MUNDIAUDIT**, por lo que deberán asumir las siguientes obligaciones:

- No difundir ninguna información relativa a los servicios proporcionados a **MUNDIAUDIT** sin autorización expresa para ello.
- Informar y difundir a su personal las obligaciones establecidas en esta Política.
- Aplicar las medidas estipuladas por RGPD en el tratamiento de los datos personales responsabilidad de **MUNDIAUDIT** que traten por razón de la prestación del servicio.
- Aplicar los procedimientos para la gestión de seguridad relacionados con los servicios proporcionados a **MUNDIAUDIT.** Especialmente se deben aplicar los procedimientos relacionados con la gestión de usuarios, tales como notificaciones de altas y bajas, identificación de los usuarios, gestión de contraseñas, etc., en el sentido descrito en la presente política y normativa reguladora que sea de aplicación.
- Notificar cualquier incidencia o sospecha de amenaza a la seguridad de algún sistema o activo de **MUNDIAUDIT** a través de los mecanismos que se determinen, colaborando en la resolución de las mismas relacionados con los sistemas, servicios o personal de la propia entidad.
- Implantar medidas en sus propios sistemas y redes para prevenir la difusión de virus y/o código malicioso a los sistemas de **MUNDIAUDIT**. Específicamente, cualquier equipo conectado a la red corporativa de **MUNDIAUDIT** debe disponer de un antivirus actualizado preferiblemente de forma automática.
- Implantar medidas en sus propios sistemas y redes para prevenir el acceso no autorizado a los sistemas de **MUNDIAUDIT** desde otras redes. Entre otros, se deben aplicar las actualizaciones de seguridad en sus sistemas y se debe mantener un sistema cortafuegos para proteger las conexiones desde Internet y otras redes no confiables.

MUNDIAUDIT se reserva el derecho de revisar la relación con la entidad externa en caso de incumplimiento de las anteriores obligaciones.

43756771F RAUL JOAQUIN BENAVENTE (R: B35586650)

Firmado digitalmente por 43756771F RAUL JOAQUIN BENAVENTE (R: B35586650)
Fecha: 2026.01.20 14:10:09 Z