

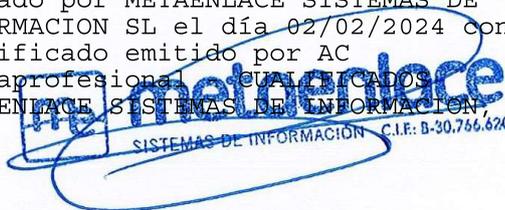
<b>PO-01</b>	<b>Revisión: 06</b>
<b>POLITICA DE CALIDAD-MEDIO AMBIENTE Y SISTEMA DE INFORMACION.</b>	<b>Fecha: 08-2020</b>
	Pág.:1 de 4

La Dirección de **METAENLACE**, declara, como Política del Sistema Integrado de Gestión de Calidad y el Medio Ambiente y para el Sistema de Gestión del Servicio y la Seguridad de la Información, lo siguiente:

**Sistema de Gestión de Calidad y Medio Ambiente:**

- **METAENLACE** es consciente de las expectativas generadas en la sociedad actual por los temas medio ambientales, por lo que, para mejorar su nivel profesional, considera imprescindible incorporar el compromiso de cumplir los requisitos de calidad y medio ambiente mediante la implantación de un **Sistema**, que deberá seguir todo su personal.
- **METAENLACE** desea lograr, dentro del marco contractual establecido, la máxima satisfacción de su clientela y el respeto al medio ambiente, incluyendo la prevención de la contaminación- en los trabajos realizados.
- **METAENLACE** asume ante su clientela un compromiso de confidencialidad de toda la documentación relativa a todos los aspectos relacionados con los trabajos desarrollados.
- **METAENLACE** pretende ser líder en los servicios que ofrece y para ello asume el compromiso firme de mejora continua en la cultura de la calidad, entendida como satisfacción al cliente y el respeto al medio ambiente, tanto para su personal, como quienes colaboren con METAENLACE o para la sociedad en general, todo ello en base al desarrollo del **Sistema**.
- **METAENLACE** cumple con la legislación y reglamentación aplicables a su actividad, así como con los requisitos y recomendaciones que se consideren necesarias, dentro del entorno de dicho **Sistema**.
- El **Sistema** incluye como referencia el marco de las normas ISO9001 e ISO14001.
- La Dirección de **METAENLACE** asume la responsabilidad de que el **Sistema** esté suficientemente documentado, comunicado a su personal y a la sociedad, manteniéndolo al día y promoviendo la participación del personal, quienes colaboren y la sociedad en general. Para ello se compromete a aportar los recursos necesarios en información, formación y sensibilización.
- **METAENLACE** se compromete con la protección del medio ambiente, la prevención de la contaminación, el uso sostenible de los recursos y la mitigación del cambio climático.

Firmado por METAENLACE SISTEMAS DE INFORMACION SL el día 02/02/2024 con un certificado emitido por AC Firmaprofesional, S.L. METAENLACE SISTEMAS DE INFORMACION, S.L. C.I.E: B-30.766.620

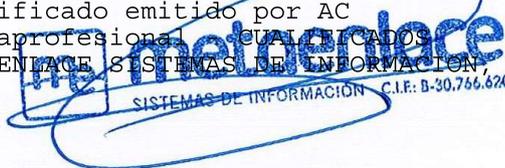


<b>PO-01</b>	<b>Revisión: 06</b>
<b>POLITICA DE CALIDAD-MEDIO AMBIENTE Y SISTEMA DE INFORMACION.</b>	<b>Fecha: 08-2020</b>
	Pág.:2 de 4

**Sistema de Gestión del Servicio y Seguridad de la Información (Sistema de Información):**

- El **objetivo** del Sistema de Información es asegurar la continuación de negocio de **METAENLACE** y minimizar los riesgos mediante la prevención de incidentes de seguridad y la reducción de su impacto potencial.
- **METAENLACE**, ha desarrollado la presente Política como la más adecuada para la prestación de los servicios recogidos en el “Catálogo de Servicios”.
- **METAENLACE** desea lograr, dentro del marco contractual establecido, la máxima satisfacción de su clientela con respecto a los servicios prestados.
- **METAENLACE** asume el compromiso de mejora continua de la eficacia del Sistema de Información y de los servicios prestados a través de la política de mejora continua establecida en el Alcance del Sistema de Información.
- **METAENLACE** se compromete a llevar a cabo, en las reuniones de Revisión del Sistema por la Dirección, el establecimiento y revisión de los objetivos de gestión del servicio y de los criterios de evaluación de las oportunidades de mejora.
- **METAENLACE** asume ante su clientela un compromiso de confidencialidad de toda la documentación relativa a todos los aspectos relacionados con los trabajos desarrollados.
- **METAENLACE** cumple con la legislación y reglamentación aplicables a su actividad, así como con los requisitos y recomendaciones que se consideren necesarias, dentro del entorno de dicho Sistema de Información.
- La Dirección de **METAENLACE** asume la responsabilidad de que el Sistema de Información esté suficientemente documentado, comunicado y entendido por su personal. Para ello se compromete a aportar los recursos necesarios en información, formación y sensibilización.
- Otro de los **objetivos de esta política** es asegurar los activos de información de la organización contra las amenazas accidentales o deliberadas, tanto internas como externas.
- Tanto la detección de amenazas y vulnerabilidades, como la estimación del riesgo intrínseco se realizará mediante reuniones periódicas en las que se evaluará el

Firmado por METAENLACE SISTEMAS DE INFORMACION SL el día 02/02/2024 con un certificado emitido por AC Firmaprofesional, S.L. **METAENLACE SISTEMAS DE INFORMACION, S.L.**



<b>PO-01</b>	<b>Revisión: 06</b>
<b>POLITICA DE CALIDAD-MEDIO AMBIENTE Y SISTEMA DE INFORMACION.</b>	<b>Fecha: 08-2020</b>
	Pág.:3 de 4

- La dirección, mediante la elaboración e implantación del Sistema de Información se **asegurará** de que:
  - *la información es protegida de accesos no deseados,*
  - *se mantiene la integridad de la información,*
  - *la confidencialidad de la información es obligatoria,*
  - *la disponibilidad de la información cumplirá los requerimientos de negocio,*
  - *se cumplen con los requisitos legales, en especial en lo relacionado con la protección de datos personales,*
  - *se desarrollarán, mantendrán y comprobarán planes de continuidad de negocio,*
  - *el personal será formado para ser consciente de sus funciones y obligaciones en lo que respecta a seguridad de la información,*
  - *los incidentes de seguridad serán obligatoriamente reportados, y serán posteriormente evaluados,*
  - *el SGSI será revisado y en concreto esta política de seguridad para mantenerla continuamente actualizada y adecuada a unas necesidades en continuo cambio.*
  
- La Dirección de **METAENLACE** consciente de la importancia de desarrollar una correcta gestión de cambios, se compromete a establecer una sistemática que garantice el control de los elementos de configuración que precisen de dicho control, así como los criterios para llevarlos a cabo, con el propósito de conseguir un mayor impacto de sus servicios ante su clientela.
  
- Para el cumplimiento de dicha Política de gestión de cambios METAENLACE establece que los componentes y elementos que están bajo el control del proceso de gestión de cambios son:

En la seguridad de la información.

En el catálogo de servicios.

En los acuerdos de nivel de servicios

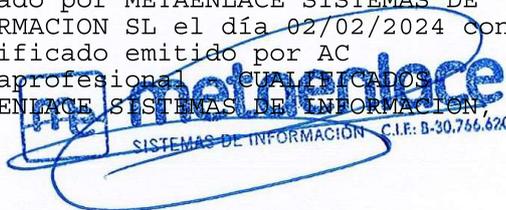
Cambios de emergencia

En infraestructuras.

Asimismo, METAENLACE ha establecido dos tipos de cambios los normales y los de emergencia. Los primeros están regulados en el proceso PSI 02 Gestión de cambios y los segundos a través del PSI 11

➤ Todo el personal de METAENLACE deberá cumplir las directrices, normas y procedimientos de esta Política de Calidad y Seguridad y del Manual de Gestión de la Información, y como consecuencia

Firmado por METAENLACE SISTEMAS DE INFORMACION SL el día 02/02/2024 con un certificado emitido por AC Firmaprofesional, S.L. METAENLACE SISTEMAS DE INFORMACION, S.L. C.I.E: B-30.766.620



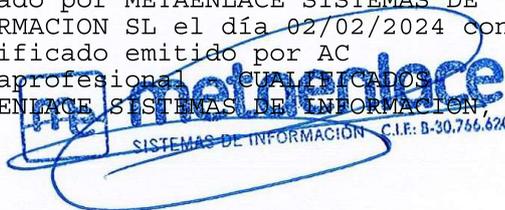
<b>PO-01</b>	<b>Revisión: 06</b>
<b>POLITICA DE CALIDAD-MEDIO AMBIENTE Y SISTEMA DE INFORMACION.</b>	<b>Fecha: 08-2020</b>
	Pág.:4 de 4

de ello asumirá el deber de ccción con esta organización en el interés de que no se produzcan alteraciones o violaciones de estas reglas.

- **METAENLACE** promoverá todos los sistemas de de Calidad-Medio Ambiente y Sistemas de Información y todas las polícias y aquellos procedimientos y protocolos necesarios, teniendo en cuenta la legislación vigente en temas de igualdad y no discriminación, así mismo promoverá la realización y mantenimiento de un Plan de Igualdad en la empresa que vele por la igualdad en la plantilla y evite el acoso o discriminación por cualquier razón, establecimiento las medias adecuadas para su comunicación y cumplimiento.
- **METAENLACE** estará legitimada en caso de comisión de alguno de los delitos o faltas tipificados por el Código Penal vigente, o en caso de observar cualesquiera conductas que a su juicio resulten contrarias a esta política, la Ley, las normas establecidas, o puedan perturbar su buen funcionamiento, imagen, credibilidad y/o prestigio, a la reclamación de los daños y perjuicios de toda naturaleza que pueda sufrir, con ocasión o como consecuencia del incumplimiento de cualquiera de las obligaciones anteriormente expuestas.
- **METAENLACE** revisa la política del **Sistema de Información**, bien anualmente, o bien ante un cambio o modificación significativa en su estructura organizativa, y se asegura que la política es apropiada.

**Fdo: GERENTE**

Firmado por METAENLACE SISTEMAS DE  
INFORMACION SL el día 02/02/2024 con un  
certificado emitido por AC  
Firmaprofesional, CUALIFICADOS  
METAENLACE SISTEMAS DE INFORMACION, S.L.  
SISTEMAS DE INFORMACION C.I.E: B-30.766.620



## Desempeño Medioambiental

**METAENLACE** es consciente de su responsabilidad con el medio ambiente en el desarrollo de su actividad, siendo un aspecto fundamental, dentro de la estrategia empresarial, la contribución a la conservación de los recursos naturales y el desarrollo sostenible.

Con el fin de cumplir con nuestro objetivo global de máximo respeto al medio ambiente, **METAENLACE** realiza diferentes actuaciones a lo largo de los últimos años, basado en riesgos y la perspectiva de ciclo de vida a todos nuestros procesos, así como al contexto de nuestra organización.

Por otra parte, desde **METAENLACE**, también hacemos partícipes a nuestros proveedores de dicho objetivo de protección al medioambiente, informándoles de nuestros requisitos de cumplimiento en este sentido para ser suministradores de productos o servicios.

Nuestros compromisos se basan principalmente en:

- Que nuestros proveedores estén localizados cerca de los centros de trabajo para reducir la huella de carbono el máximo posible.
- Que reduzcamos la emisión de CO2 a la atmosfera por trabajador, emitiendo un máximo de 163,5kg de CO2 por personal.

Fdo. GERENTE

## INDICE 1

<b>1. APROBACIÓN Y ENTRADA EN VIGOR.....</b>	<b>2</b>
<b>2. INTRODUCCIÓN .....</b>	<b>2</b>
<b>3. PRINCIPIOS Y DIRECTRICES.....</b>	<b>3</b>
3.1. PREVENCIÓN .....	3
3.2. DETECCIÓN .....	4
3.3. RESPUESTA .....	4
3.4. RECUPERACIÓN .....	5
<b>4. ALCANCE .....</b>	<b>5</b>
<b>5. MISIÓN .....</b>	<b>7</b>
<b>6. MARCO NORMATIVO.....</b>	<b>7</b>
<b>7. ORGANIZACIÓN DE LA SEGURIDAD .....</b>	<b>8</b>
<b>8. ESTRUCTURA, ROLES Y RESPONSABILIDADES .....</b>	<b>8</b>
<b>8.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>8</b>
8.1.1. CONSTITUCIÓN.....	8
8.1.2 FUNCIONES Y RESPONSABILIDADES DEL COMITÉ.....	9
<b>8.2. RESPONSABLES Y MIEMBROS DEL COMITÉ .....</b>	<b>11</b>
8.2.1 Responsable de la Información y de los Servicios.....	11
8.2.2 Responsable de Seguridad .....	11
8.2.3 Responsable del Sistema.....	12
<b>8.3. PROCEDIMIENTOS DE DESIGNACIÓN .....</b>	<b>13</b>
<b>8.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>13</b>
<b>9. DATOS DE CARÁCTER PERSONAL.....</b>	<b>14</b>
<b>10. GESTIÓN DE RIESGOS.....</b>	<b>14</b>
<b>11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>15</b>
<b>12. OBLIGACIONES DEL PERSONAL.....</b>	<b>15</b>
<b>13. TERCERAS PARTES .....</b>	<b>16</b>

Firmado por \*\*\*9123\*\* PEDRO MUÑOZ (R:  
\*\*\*\*6662\*) el día 19/01/2024 con un  
certificado emitido por AC  
Representación

METAENLACE SISTEMAS DE INFORMACION,  
S.L.

Esta documento es propiedad de METAENLACE  
Queda prohibida su reproducción total o parcial sin consentimiento de la propia organización.

## 1. APROBACIÓN Y ENTRADA EN VIGOR

Texto revisado por el Responsable de Seguridad de Metaenlace y aprobado el día 19 de enero de 2024 por el Comité de Seguridad de la Información incluyendo la nueva figura del POC y actualizando la legislación aplicable.

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

## 2. INTRODUCCIÓN

Metaenlace es una empresa de servicios integrales para sistemas de información, que comprenden desde consultoría tecnológica hasta ingeniería e integración de sistemas. Constituida en 2001, ha conseguido excelentes resultados en diversas vertientes, destacando especialmente en la creación de sistemas de información a medida. En Metaenlace disponemos de una amplia solvencia técnica, profesional y financiera, para abordar proyectos de envergadura, y que viene avalada por su dilatada experiencia en la prestación de numerosos y complejos servicios para sistemas de información. Esta solvencia ha permitido que en los últimos años nos hayamos posicionado como uno de los proveedores de referencia tanto de la Administración pública, como de las grandes empresas privadas a nivel nacional, sin perder por ello la cercanía y el trato personal con nuestros clientes.

Colaboramos con la Administración pública en la mejora y mantenimiento de sus procesos y sistemas de gestión. Pioneros en el Programa '0 Papel', somos especialistas en Administración electrónica, facilitando el acceso de los ciudadanos a todo tipo de trámites burocráticos y gestión documental a través de internet.

Metaenlace ha desarrollado con éxito importantes proyectos en áreas tan sensibles como Educación, Sanidad, Hacienda y Tributos, con iniciativas que repercuten de forma favorable, aumentando y mejorando los servicios que reciben los ciudadanos.

El sector privado requiere que el enfoque de concepción de los procesos y sistemas de información evolucionen y se adapten a un mundo cada vez más competitivo y cambiante.

Nuestra experiencia nos permite desarrollar proyectos para grandes empresas y corporaciones, estableciendo el control de los procesos y la centralización de la información durante todas las fases del ciclo de vida del producto, desde el diseño a la construcción, pruebas, mantenimiento, evolución, etc., en sectores de vital importancia para la economía como son la banca, industria petroquímica, la gran industria textil...

**METAENLACE** depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para prestar sus servicios. A tenor de ello los sistemas deben ser administrados 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 o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada 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 se deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

METAENLACE debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes.

### **3. PRINCIPIOS Y DIRECTRICES**

#### **3.1. PREVENCIÓN**

METAENLACE debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementa las medidas

mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, METAENLACE:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

### **3.2. DETECCIÓN**

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios se monitorizan de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en RD 311/2022 del ENS.

Se establecen mecanismos de detección, análisis y reporte que llegan a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

### **3.3. RESPUESTA**

METAENLACE:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto 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).(Protocolo de Sistemas/Plan de Continuidad)

### **3.4. RECUPERACIÓN**

Para garantizar la disponibilidad de los servicios críticos, METAENLACE ha desarrollado un Plan de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

### **4. ALCANCE**

Esta Política se aplica a los sistemas TIC de METAENLACE que se encuentran dentro del alcance del Esquema Nacional de Seguridad y a todos los miembros de la organización, sin excepciones. También se aplica sobre personal en prácticas y personal externo que puedan participar en los procesos de negocio de manera directa o indirecta.

El alcance del Sistema de Gestión de Seguridad de la Información es

Los sistemas de información que dan soporte a los procesos de negocio según la declaración de aplicabilidad en vigor de:

- Consultoría (estudio y asesoramiento de la situación, del entorno, del uso, de la aplicación y de la influencia) de tecnologías de la información.
- Realización, implantación y mantenimiento preventivo, evolutivo y correctivo de Sistemas de información.
- Mantenimiento, reparación, venta, asistencia técnica y gestión de incidencias en Sistemas de Información.

Dichos servicios se prestan a través del plan de gestión, según correspondan, desde su sede principal y/o en el domicilio del cliente, empleando para ello la tecnología recogida a continuación:

- Sistemas y programas
- Sistemas operativos cliente-servidor, aplicaciones de ofimática, aplicación Metagest, Repositorio de Gestión de Versiones, etc.

- Sistemas Informáticos (Hardware)
- Servidores, PCs de sobremesa, Impresoras, escáneres, sistemas de comunicación (redes y telefonía), soportes de almacenamiento externo, Sistemas de Alimentación Ininterrumpida, etc.

Los distintos activos recogidos en el alcance del sistema de información están recogidos en el archivo “Inventario de activos” donde además se analizan sus riesgos, vulnerabilidades, criticidad y controles.

El sistema de información abarca en cuanto a seguridad, todos y cada uno de los procesos en el Mapa de procesos recogidos por Metaenlace así como a todos los departamentos y áreas establecidos en su organigrama.

La Política de Seguridad es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

**1.Primer nivel: Política de Seguridad de la Información.**

Constituye el primer nivel la Política de Seguridad de la Información, recogida en el presente texto. La Política de Seguridad requiere la aprobación por parte del Responsable de Seguridad

**2.Segundo nivel: Normativa de Seguridad de la Información.**

El segundo nivel desarrolla la Política de Seguridad de la Información mediante procedimientos específicos que abarcan un área o aspecto determinado de la seguridad de la información. La documentación se estructura en procedimientos y son aprobados por el Responsable de seguridad.

**3.Tercer nivel: Procedimientos de Seguridad de la Información.**

El tercer nivel está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios.

Los procedimientos y políticas son aprobados por el Responsable de Seguridad de la Información.

El personal de METAENLACE tiene la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Políticas y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones.

La Política, las Políticas específicas y los Procedimientos de Seguridad de la información están disponibles en el correo del usuario y en la Intranet de la organización.

## 5. MISIÓN

En METAENLACE somos conscientes que todas las empresas tienen diferentes necesidades y problemáticas a solucionar.

Es por esto que, como expertos, nos apoyamos en nuestro conocimiento y bagaje profesional, para ofrecer soluciones que cubran estas necesidades rentabilizando al máximo las inversiones.

## 6. MARCO NORMATIVO

A continuación, se detalla el marco normativo que debe cumplir la organización:

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual.

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

## 7. ORGANIZACIÓN DE LA SEGURIDAD

Mediante la estructuración de nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión se base en los siguientes documentos:

- Documentos Internos: los generados por el propio sistema de gestión.
- Documentos Externos: documentos necesarios para el correcto desarrollo del SGSI, no elaborados por la METAENLACE. como: legislación, normas, etc. Y además existen dos tipos de registros:
  - Registros internos: los generados por el propio SGSI.
  - Registros externos: registros recibidos del exterior (clientes, administración, proveedores, ...)

## 8. ESTRUCTURA, ROLES Y RESPONSABILIDADES

### 8.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

#### 8.1.1. CONSTITUCIÓN

El Comité presenta estructura orgánica y está formado por delegados de las partes interesadas en la óptima gestión de la Seguridad de la Información. La postura oficial del Comité ante cuestiones sometidas a votación será delimitada por mayoría simple.

Los integrantes del Comité de Seguridad de la Información se detallan en la siguiente tabla.

---

#### COMITÉ SEGURIDAD DE LA INFORMACIÓN

DEPARTAMENTO	NOMBRE	FUNCION	REPONSABILIDAD	
Gerencia	Pedro Muñoz	Presidente	Responsable de la información	
Gerencia	Rosario Ibañez Barnes	Vocal	Responsable del servicio	
Responsable	Bernardo Muñoz	Secretario	Responsable de seguridad	seguridad.ens@metaenlace.com
			POC	
Sistemas	Antonio Sánchez	Vocal	Responsable del sistema	sisistemas.ens@metaenlace.com

El secretario del Comité tiene como funciones del cargo:

- Convocar las reuniones del Comité.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el Acta de Reunión.
- Impulsar la ejecución directa o delegada de las decisiones del Comité.

El Presidente del Comité es responsable de presidir las reuniones. Así mismo, será responsable de revisar las Actas de Reunión y aprobarlas formalmente con su firma.

### 8.1.2 FUNCIONES Y RESPONSABILIDADES DEL COMITÉ

- Atender las solicitudes que, en materia de Seguridad de la Información, formulen el resto de órganos o unidades del Ayuntamiento, informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los distintos departamentos o responsables.

- Promover la mejora continua del sistema de gestión de la Seguridad de la Información, para lo que se encargará de:
  - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, asegurando que sean consistentes y estén alineados con la estrategia decidida en la materia, y evitar duplicidades.
  - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
  - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
  - Realizar un seguimiento de los principales riesgos residuales asumidos por el Ayuntamiento y recomendar posibles actuaciones respecto de ellos.
  - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
  - Elaborar y revisar regularmente la Política de Seguridad de la Información para su ulterior aprobación por el órgano competente.
  - Aprobar las Normativas y Procedimientos de Seguridad de la Información.
  - Aprobar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
  - Aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
  - Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

## 8.2. RESPONSABLES Y MIEMBROS DEL COMITÉ

### 8.2.1 Responsable de la Información y de los Servicios

- Establecer y proponer para aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a los servicios y la información comprendidos en el ámbito de la Política de Seguridad de la Información de la entidad.
- Proponer para aprobación al Comité de Seguridad de la Información de los niveles de riesgo residual que afecten a los antedichos Servicios y a la Información.

### 8.2.2 Responsable de Seguridad

- Determinar las medidas de seguridad de naturaleza técnica que deberán ser implantadas para alcanzar las valoraciones realizadas por los Responsables de la Información y los Servicios.
- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Determinar la categoría del sistema, en colaboración con el Responsable del Sistema, para su eventual aprobación por el Comité de Seguridad de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las auditorías y revisiones, externas o internas, de la seguridad del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

- Podrá desplegar otras funciones derivadas de otras normas jurídicas de aplicación, siempre que concurren los requisitos de conocimiento, experiencia, independencia y en su caso titulación.
- Ejercer de POC con las Administraciones Públicas con las que se trabaje.

### 8.2.3 Responsable del Sistema

- Detener cautelarmente la prestación de los servicios o suspender cautelarmente el acceso a la información si tiene el conocimiento de que estos presentan deficiencias graves de seguridad que pudiera ser atacadas de forma inminente, informando de ello a la presidencia del Comité de Seguridad de la Información.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al Responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema, en el caso de no estar designado explícitamente dicho rol.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.

- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

### **8.3. PROCEDIMIENTOS DE DESIGNACIÓN**

La designación de los Responsables identificados en esta Política ha sido realizada por el el Comité de Seguridad de la Información. El nombramiento será indefinido y se revisará cuando el puesto quede vacante. En este último caso será necesario realizar el nombramiento en el plazo de un mes. La presidencia del comité será nombrada por la Dirección General de la empresa, mientras que la figura de Secretario corresponderá a la persona Responsable de la Seguridad del Esquema Nacional de Seguridad.

### **8.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

Será misión del Comité de Seguridad de la Información 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 el Comité de Seguridad y difundida para que la conozcan todas las partes afectadas.

La difusión se practicará vía e-mail, a todos los trabajadores de la empresa, indicando la ubicación del texto definitivo de la Política en el portal WEB.

## 9. DATOS DE CARÁCTER PERSONAL

METAENLACE trata datos de carácter personal. El documento "Registro de Actividades de Tratamiento" al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados, los responsables correspondientes y las actividades de tratamiento realizadas.

Todos los sistemas de información de METAENLACE. se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado "Registro de Actividades de Tratamiento".

## 10. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- 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 de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

## **11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

Esta Política de Seguridad de la Información complementa las políticas de seguridad de METAENLACE aplicadas en materia de Protección de Datos de Carácter Personal.

Esta Política se desarrollará por medio de los procedimientos y políticas 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.

La normativa de seguridad estará disponible en la intranet:

En la capeta compartida ubicada en el Servidor denominada "Calidad".

## **12. OBLIGACIONES DEL PERSONAL**

Todos los miembros de METAENLACE 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 TIC disponer los medios necesarios para que la información llegue a los afectados.

Se ha establecido un programa de concienciación continua para atender a todos los miembros, 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. TERCERAS PARTES**

Cuando METAENLACE preste servicios a terceros o maneje información de otros, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte, coordinación y procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando METAENLACE utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

En Murcia a 19 de enero de 2024