MASTERTEC

PLS-ENS-001

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

**PÚBLICO**


ens
Esquema Nacional de
Seguridad

**CONTROL DEL DOCUMENTO**

| | |
|---|---|
| Nombre del documento: **MASTERTEC-PLS-ENS-001-Política Seguridad de la Información-V01.docx**<br>Número de Páginas: **13** | |
| Autor: Responsable de Seguridad | |
| **Aprobado por Dirección a fecha de firma electrónica** | **Firma:** |
| Clasificación de la información: **PÚBLICO** | |
| Lista de distribución: SIN RESTRICCIONES | |

Este documento está dirigido EXCLUSIVAMENTE a las personas nombradas en la lista de distribución, las cuales podrán, en base a su criterio, divulgarlo a los que consideren oportuno. Se recomienda encarecidamente una divulgación controlada donde todos los cesionarios del documento conozcan inequívocamente su CLASIFICACIÓN y se comprometan a mantener la consecuente confidencialidad en todo el ciclo de uso y, en su caso, archivo y/o destrucción.

**CONTROL DE VERSIONES**

| Núm. Versión | Autor | Fecha | Cambios realizados | Comentarios |
|---|---|---|---|---|
| 1.0 | Responsable de Seguridad | 21/11/2023 | Versión Inicial | Sin Comentarios |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# POLÍTICA DE SEGURIDAD

## Índice

# 1) APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 21 de noviembre 2023

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde la fecha mencionada y hasta que sea reemplazada por una nueva Política.

# 2) INTRODUCCIÓN

Las empresas del **Grupo Mastertec: Mastertec S.A.** y **STM Mantenimiento S.L.** (en adelante solo MASTERTEC), dependen de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos ante daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o a los servicios prestados.

El objetivo de la seguridad de la información es garantizar la confidencialidad, integridad, autenticidad y trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con premura a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, la integridad, la disponibilidad, el uso previsto y el valor de la información y los servicios. Para defenderse de estas amenazas, es necesaria una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continuada de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como hacer 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.

Los diferentes departamentos deben asegurarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde la concepción hasta el retiro de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y la valoración de su coste deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

# 3) MISIÓN

MASTERTEC siempre ha acompañado a las empresas en su transformación digital a través de todas las necesidades tecnológicas imaginables. Desde los primeros programas artesanales hasta la tecnología más avanzada, hemos enfocado nuestra misión en el soporte y asesoramiento a las empresas del territorio.

Ahora, con la segunda generación en la dirección, queremos potenciar más, si cabe, este enfoque hacia el servicio trabajando duramente para defender los valores de confianza, profesionalidad, seguridad y proximidad que siempre hemos defendido.

Afrontamos esta visión con determinación, consciente de la enorme complejidad que supone el futuro de la tecnología e ilusionados permanentemente para continuar encontrando las soluciones a los retos que se nos presenten.

# 4) ALCANCE

Esta Política se aplicará a los sistemas de información de MASTERTEC, que dan soporte a las actividades de los servicios siguientes:

- Soporte y mantenimiento de material tecnológico y artes gráficas

- Distribución de material tecnológico y artes gráficas

# 5) MARCO NORMATIVO

Los marcos normativos referenciales se encuentran en el Registro Corporativo de Marcos Normativos:

**MASTERTEC-RGS-GLB-002-Normativa Aplicable**

Conteniendo los marcos normativos aplicables a MASTERTEC

# 6) CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS DE SEGURIDAD

MASTERTEC, para alcanzar el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que recoge los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

**La seguridad como un proceso integral y mínimo privilegio**

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad en MASTERTEC, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se debe prestar la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que la ignorancia, la falta de organización y coordinación o instrucciones inadecuadas constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para el correcto ejercicio, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance los objetivos competenciales o contractuales.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo las desarrollan las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas para el objetivo que se persigue. El uso ordinario del sistema debe ser sencillo y seguro, de manera que una utilización insegura requiera un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, para eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

**Vigilancia continua, re-evaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad**

La vigilancia continua por parte de MASTERTEC permitirá la detección de actividades o comportamientos anómalos y la respuesta oportuna.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se re-evaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuera necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y la monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de manera continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

**Gestión de personal y profesionalidad**

Todo el mundo, propio o ajeno relacionado con los sistemas de información de MASTERTEC, dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y el alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De la misma manera, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo del puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases del ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

**Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos**

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continuada y permanentemente actualizada.

La gestión de los riesgos permitirá mantener un entorno controlado y minimizar los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una aplicación apropiada de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a que estén expuestos.

Esta gestión se realizará por medio del análisis y el tratamiento de los riesgos a que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se utilizará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deben estar justificadas y, en todo caso, hay una proporcionalidad entre ellas y los riesgos.

**Incidentes de seguridad, prevención, detección, reacción y recuperación**

Mastertec dispone de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de las vías de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, con el fin de minimizar las vulnerabilidades y conseguir que las amenazas sobre éste no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

Del mismo modo, el sistema mantendrá los servicios disponibles durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

**Existencia de líneas de defensa y prevención frente a otros sistemas de información interconectados**

Mastertec ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de manera que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada ante los incidentes que no se han podido evitar, reduciendo la probabilidad de que el sistema sea comprometido en conjunto y minimizar su impacto final.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema de MASTERTEC se conecta a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará el punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la instrucción técnica de seguridad correspondiente.

**Diferenciación de responsabilidades, organización e implantación del proceso de seguridad**

Mastertec ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "MODELO DE GOBERNANZA" del presente documento.

**Autorización y control de los accesos**

MASTERTEC ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

**Protección de las instalaciones**

Mastertec ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

**Adquisición de productos de seguridad y contratación de servicios de seguridad**

Para la adquisición de productos o contratación de servicios de seguridad, MASTERTEC, tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

**Protección de la información almacenada y en tráfico y continuidad de la actividad**

Mastertec prestará especial atención a la información almacenada o en tráfico a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para conseguir una adecuada protección.

Deben aplicarse procedimientos que garanticen la recuperación y la conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este Real Decreto, cuando sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a que se refiere este Real Decreto, deberá estar protegida con el mismo grado de seguridad que la misma. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que sean aplicables.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

**Registro de actividad y detección de código nocivo**

Mastertec, con el propósito de satisfacer el objeto de este Real Decreto, con garantías plenas del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que sean aplicables, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Con el fin de preservar la seguridad de los sistemas de información y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, MASTERTEC podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de manera que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código nocivo así como otros daños en las redes y sistemas de información mencionadas.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de manera única, de manera que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

**Infraestructuras y servicios comunes**

MASTERTEC, tendrá en cuenta que la utilización de infraestructuras y servicios comunes de la organización, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto.

**Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras**

Mastertec tendrá en cuenta la aplicación de los perfiles de cumplimiento específicos publicadas por el CCN.

# 7) MODELO DE GOBERNANZA

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información en MASTERTEC, designará roles de seguridad y constituirá un Comité de Seguridad de la información.

## 7)1. Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, de la siguiente manera:

- **Responsable/s de información:** Comité de Seguridad de la Información
- **Responsable de los Servicios:** Comité de Seguridad de la Información
- **Responsable de Seguridad:** Responsable de Informática Grupo Mastertec
- **Responsable del Sistema:** Responsable de Informática Grupo Mastertec

## 7)2. Comité de Seguridad de la Información

Se ha constituido un Comité de Seguridad de la Información, como órgano colegiado, y está formado por los siguientes miembros:

| Cargo en el Comité | Cargo Corporativo |
|---|---|
| Presidencia | Gerente Grupo Mastertec |
| Secretaría | Responsable de Seguridad |
| Vocal 1 | Responsable RRHH Mastertec |
| Vocal 2 | Responsable RRHH STM |
| Vocal 3 | Responsable Jurídico / DPD Grupo Mastertec |

Los responsables de la información y de los servicios serán convocados en función de los asuntos a tratar.

Asimismo, y con carácter opcional, se pueden incorporar a las tareas del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

Los miembros del Comité serán renovados cada cuatro años o con motivo de vacante.

## 7)3. Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

### **7)3.1.** Funciones del Responsable de la Información y de los Servicios

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto del Esquema Nacional de Seguridad.
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

### **7)3.2.** Funciones del Responsable de Seguridad

- 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 las configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el responsable del sistema.
- 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 revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.

### 7)3.3. Funciones del Responsable del Sistema

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- 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.
- Asegurarse 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, en su caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, si procede, del hardware y software en 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 estrictamente cumplidos.
    - 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 los mecanismos de auditoría técnica.

## 7)4. Funciones del Comité de Seguridad de la Información

Las funciones propias de un Comité de Seguridad de la Información son las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de la administración y de los diferentes roles de seguridad y/o áreas 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 las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la seguridad de la información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

- Proponer planes de mejora de la Seguridad de la Información, con la dotación presupuestaria correspondiente, y priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar por que la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta la 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 la Administración y recomendar posibles actuaciones.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de estos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para aprobarla el órgano competente.
- Elaborar la normativa de Seguridad de la Información para aprobarla en coordinación con la Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar 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.
- Elaborar y 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 compañía en materia de seguridad de la Información.

## 7)5. Procedimientos de designación

La designación de los Responsables identificados en esta Política ha sido realizada por el Consejo de administración del Grupo MASTERTEC, y comunicada a las partes afectadas mediante aceptación formal del cargo.

Los roles de seguridad serán revisados cada cuatro años. En caso de que haya una vacante, ésta deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

## 7)6. Resolución de conflictos

Si hay conflicto entre los responsables, será resuelto por el Comité de Seguridad de la Información.

# 8) DATOS DE CARÁCTER PERSONAL

Mastertec, en el tratamiento de los datos personales, cumple los principios y obligaciones de la normativa vigente, entre otra el Reglamento 679/2016, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos y por lo que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos-RGPD-) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, respetando, en todo

caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

# 9) DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas y los procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad. Para nuestra organización se ha definido una Norma para la Gestión de la Documentación, que establece las directrices para la organización, la gestión y el acceso.

La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información proponiendo en caso de que sea necesaria mejoras de esta, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

# 10)TERCERAS PARTES

Cuando lo presta servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Mastertec definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que Mastertec lleve a cabo en materia de seguridad en relación con otros organismos.

Cuando MASTERTEC, utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que afecta a estos servicios o información. Esta tercera parte queda sujeta a las obligaciones establecidas en la normativa mencionada, y pueden desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el que establece esta Política de Seguridad.

Del mismo modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiera en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que necesite los riesgos en que se incurre y la manera de tratarlos. Este informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.