# Política de Seguridad de TELECONTROL STM, S.L.

| Estado de revisiones | Descripción de motivos |
|---|---|
| Rev 0 | **Creación del documento 2013** |
| Rev 1 | **Diciembre 2015:**<br><br>**Se actualiza el documento adaptándolo a las nuevas exigencias** |

Cristina Domínguez Encinas
Rev. 1 29/01/20165

Departamento de Administración y Control

# Índice

## 1. ALCANCE

El alcance del siguiente documento va dirigido a todos los trabajadores de la empresa TELECONTROL STM, S.L., con el fin de facilitar y entender, la manera de actuar ante el tratamiento o manejo del Sistema de Información en la empresa, así como el manejo, conocimiento o tratamiento de datos de carácter personal de los trabajadores que la integran.

## 2. GLOSARIO DE TÉRMINOS

### 1. Acceso

Acción mediante la cual un usuario entra en un determinado recurso, (local, sistema de información, equipo informático, red…).

### 2. Activo

Los activos son los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Ejemplos de activos pueden ser los servidores de datos, las aplicaciones informáticas o los expedientes en papel.

### 3. Actualización

Es el término que se utiliza para identificar los diferentes tipos de paquetes que pueden hacer que un sistema esté al día y/o incluya nuevas funcionalidades.

### 4. Amenaza

Evento que puede producir un daño en el sistema de información.

### 5. Antivirus

Software para la detección y prevención de virus.

### 6. Auditoría

Proceso de obtención y análisis de evidencias a fin de su evaluación y la elaboración de un informe acerca de la fiabilidad de los registros analizados.

### 7. Autenticación

Proceso mediante el cual se comprueba la identidad de un usuario.

### 8. Autorización

Derecho otorgado a un individuo autenticado o proceso para utilizar el sistema de información y la información que éste contiene.

9. Certificado Digital

Sistema de acreditación que contiene información de un usuario o servidor, para la verificación de su identidad en el sistema de información.

10. Cesión de Datos

Toda revelación de datos realizada a una persona distinta del interesado.
No se considera cesión de datos cuando el acceso sea necesario para la prestación de un servicio al responsable del fichero.

11. Código malicioso (Malware)

Hardware, software o firmware que es intencionalmente introducido en un sistema de información con un fin malicioso o no autorizado, (virus, troyanos, gusanos, rootkit…).

12. Comunicaciones

Transmisión y recepción de información que se realiza entre dos o más equipos o soportes de un sistema de información.

13. Confidencialidad

Políticas y normas para garantizar que los datos y/o documentos no sean tratados ni comunicados de manera incorrecta ni a los trabajadores ni a personas no autorizadas.

14. Contraseña

Cadena de caracteres que un usuario o servicio utiliza para verificar su identidad frente a un equipo, soporte o sistema de información.

15. Control de Acceso

Mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos de un sistema de información, dejando un registro de dicho acceso.

16. Controles Físicos

Medidas de seguridad que vigilan y registran accesos físicos a un sistema de información.

17. Controles Lógicos

Conjunto de principios y normas que vigilan y registran los accesos a datos, procesos e información.

18. Datos de Carácter Personal

Cualquier información concerniente a personas físicas que las identifique o las haga identificables.

19. Disponibilidad

Garantizar que los recursos estén disponibles cuando se necesiten.

20. Dispositivo móvil

Soporte de tratamiento o almacenamiento de información extraíble y/o transportable.

21. Divulgación

La exposición de información a terceros que no tienen acceso a ella.

22. Documento de Seguridad

Documento que contiene las medidas de seguridad aplicadas por la empresa, para proteger los datos de carácter personal de accesos no autorizados.

23. Encargo de Tratamiento

Concesión de acceso a datos de carácter personal, delegando la ejecución de un servicio necesario para la relación entre el responsable de fichero y los afectados.

24. Encriptación

Proceso mediante el cual la información es codificada para evitar el acceso a la misma por terceros no autorizados.

25. Entorno

Conjunto de elementos que rodean el sistema de información de una empresa sin formar parte del mismo.

26. Evidencia

Prueba que demuestra de forma clara, manifiesta y perceptible un hecho.

27. Fichero

Conjunto organizado de datos.

28. Fichero de Datos de Carácter Personal

Conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

29. Firewall

Conjunto de hardware y software cuya función es proteger un sitio privado conectado a una red (local, intranet, Internet,…) contra accesos no autorizados.

30. Gestión

Proceso mediante el cual se obtiene, despliega o utiliza una variedad de recursos básicos para apoyar los objetivos del proceso.

31. Hacker

Experto informático especialista en entrar en sistemas ajenos sin permiso.

### 32. Incidencia

Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos del sistema de información de la empresa.

### 33. Información

Conjunto de datos que al relacionarse adquieren sentido o un valor de contexto o de cambio.

### 34. Información Confidencial

Conjunto de datos relativos a la empresa que pueda comprometer sus procesos clave. También se refiere a los datos especialmente protegidos (Ideología, religión, afiliación sindical, creencias, origen racial o étnico, salud o vida sexual).Que no podrán salir ni ser comunicados fuera de la empresa sin la autorización de su creador y/o Responsable de los ficheros, en función de su contenido.

### 35. Información Restringida

Conjunto de Datos relativos a la empresa, que solo va dirigida a una parte de la totalidad de los empleados y que no puede ser difundida a terceros por su contenido.

### 36. Información de Carácter pública

Conjunto de datos relativos a la empresa o no, que no está identificada como restringida o Confidencial y que es accesible a todo al personal de la empresa y que puede ser comunicada a terceros, bajo responsabilidad del que la difunde.

### 37. Integridad

Seguridad de que una información no ha sido alterada.

### 38. Internet

Conjunto de equipos y redes conectados a nivel mundial para el intercambio de información.

### 39. ISO 17799

Código de Buenas Prácticas de Seguridad de la Información.

### 40. Registro (Log)

Documento que recoge evidencias objetivas de las actividades efectuadas o de los resultados obtenidos en un proceso.

### 41. LOPD (Ley de protección de datos de carácter personal)

Ley 15/99, de 13 de Diciembre, de tratamiento de datos de carácter personal.

### 42. LSSI (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico)

Ley 34/2002, de 11 de Julio, de servicios de la sociedad de la información y de comercio electrónico.

### 43. Nivel de Seguridad (Básico, Medio y Alto)

Niveles de seguridad definidos en el Real Decreto 994/99, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros automatizados que contengan Datos de Carácter Personal.

### 44. Perfil de Usuario

Definición de las competencias, niveles de acceso y responsabilidades asignadas a un usuario para el desempeño de sus funciones.

### 45. Permiso

Reglas para regular qué usuarios pueden obtener acceso y de qué manera a los distintos recursos del sistema de información.

### 46. Privacidad

El control sobre el uso, comunicación y distribución de la información.

### 47. Privilegios

Derechos del usuario para utilizar los distintos activos del sistema de información.

### 48. Proceso

Conjunto de actividades o eventos que se realizan o suceden con un determinado fin.

### 49. Recurso

Cualquier componente de un sistema de información.

### 50. Red Local

El término red local incluye tanto el hardware como el software necesario para la interconexión de varios ordenadores y periféricos con el objeto de intercambiar recursos e información.

### 51. Responsable del Fichero

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento del Sistema de información en la empresa y datos de carácter personal.

### 52. Responsable de Tratamiento

Es la persona física o jurídica, autoridad pública, servicio o cualquier otro mecanismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero.

### 53. Riesgo

Probabilidad de obtener un resultado desfavorable como resultado de la exposición a un evento especifico.

### 54. RMS (Real Decreto de Medidas de Seguridad)

Niveles de seguridad definidos en el Real Decreto 994/99, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros automatizados que contengan Datos de Carácter Personal.

### 55. Salvaguarda

Tecnología, política o procedimiento que contrarresta una amenaza o protege un valor.

### 56. Seguridad

Disciplina, técnicas y herramientas diseñadas para ayudar a proteger la confidencialidad, integridad y disponibilidad de información y sistemas.

### 57. Sistema de Información Empresarial ( S.I.E.)

Conjunto de elementos, ordenadamente relacionados entre sí que aporta a la organización las directrices de manejo, tratamiento de la información y soporte necesario para el cumplimiento de sus fines, así como de su funcionamiento. Se incluyen documentos, archivos, programas, software

### 58. Software

Conjunto de programas y aplicaciones para el manejo de información en el sistema empresarial.

### 59. Soporte

Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden gravar o recuperar datos.

### 60. Terceros

Personas que no forman parte de la organización.

### 61. Tratamiento de datos

Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

### 62. Vulnerabilidad

Probabilidad de que una amenaza afecte a un activo causando un daño.

## 3. DIRECTRICES QUE DEBEN SEGUIRSE PARA CUMPLIR LA POLITICA DE SEGURIDAD EN LA EMPRESA.

- Existe una prohibición expresa del uso de los activos de la empresa, tanto recursos informáticos (correo electrónico, Internet, ofimática, espacio en disco, etc.), como información (de clientes, de terceros, etc.), para finalidades distintas a las estrictamente aprobadas por la Dirección.
- Se establecerán normas para prevenir y regular el uso de dichos servicios por parte del personal de la empresa.
- Se seguirán las medidas de seguridad definidas por la organización en el correcto desempeño de sus funciones.
- Existe la obligación por parte del usuario de bloquear los puestos de trabajo desde los que opera cuando sean abandonados, bien temporalmente o bien al finalizar el turno de trabajo. Las Contraseñas de cada usuario son intransferibles.
- La seguridad no es un producto sino un proceso, cuya implantación exige un cambio cultural y organizativo en la empresa, que debe ser liderado por la dirección.

## 4. GESTIÓN DE RECURSOS DEL SISTEMA DE INFORMACIÓN

La empresa, en la persona del responsable de los ficheros (Gerencia), es responsable de la protección de la información que gestiona ante las amenazas del entorno y debe, por todos los medios disponibles, garantizar la confidencialidad, integridad y disponibilidad del Sistema de Información que maneja, por ello las características que debe cumplir la seguridad de la Información en la empresa y que debe considerar son:

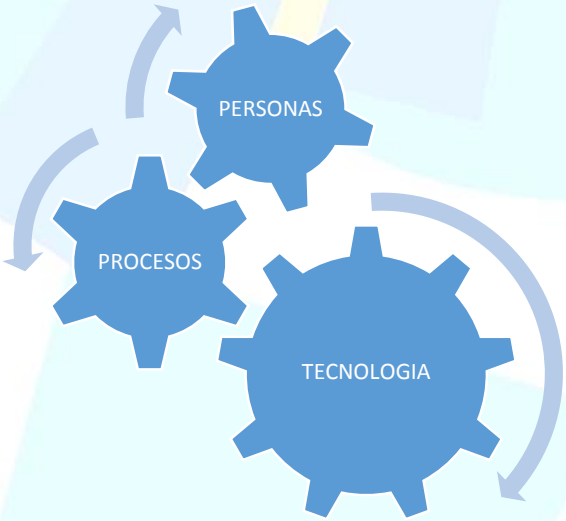
- **Disponibilidad**: asegurar que los usuarios autorizados tienen acceso cuando lo requieran en los tiempos adecuados.
- **Integridad**: garantía de la exactitud y de que la información sea completa, así como los métodos de su procesamiento.
- **Confidencialidad**: asegurar que la información es sólo accesible para aquellos Autorizados.
- **Autenticidad de los usuarios del servicio**: asegurar la identidad de los usuarios que manejan o acceden al activo.
- **Autenticidad del origen de los datos**: asegurar la identidad u origen de los datos.
- **Trazabilidad del servicio**: asegurar que en todo momento se podrá determinar quién hizo qué y en qué momento.
- **Trazabilidad de los datos**: asegurar que en todo momento se podrá determinar quién ha accedido a los datos.

Se deben detectar las situaciones que se están realizando sin control adecuado y para Ello, deben ser analizados los aspectos importantes en materia de seguridad, como la Confidencialidad de los datos de clientes o la disponibilidad de los sistemas informáticos de la empresa.

Una adecuada gestión de la seguridad de la información debe contribuir a disminuir los riesgos que la empresa soporta, y a minimizar los daños en los activos de información, si alguno de los riesgos llega a materializarse.

La Gestión de la Seguridad: introduce el término "gestión" como estrategia para abordar las actuaciones que toda organización debe realizar en materia de seguridad de la información.

Es necesario que los tres elementos funcionen de forma conjunta y coordinada:
– **Tecnología**: medidas tecnológicas de protección.
– **Procesos:** supervisar el correcto funcionamiento de la tecnología y las personas.
– **Personas**: utilizan la tecnología y ejecutan los procesos.




## 5. NORMAS PARA EL TRATAMIENTO DE LA INFORMACIÓN

El desarrollo de las actuaciones necesarias en materia de seguridad de la información, con el objeto de reducir el riesgo asociado a la pérdida o filtración de los datos de clientes y la pérdida de disponibilidad del sistema de información de la empresa, se abordará, desde las siguientes medidas:

- Se establece un sistema fácil y ágil de clasificación de la información, donde cada documento (Comunicado, carta, documento, archivo, carpeta, etc.) que forma parte del Sistema de Información interna de la empresa y que es difundido a personal interno o, deberá aparecer como "Confidencial", "Restringido" o con carácter "Publico", cuando no venga identificado, facilitando así el uso y responsabilidades en su distribución. Nos remitimos a la definición de cada uno de los términos en el Glosario.


- Se regulará mediante contrato todos los encargos de tratamiento de datos y prestación de servicios con terceros que impliquen el intercambio de información. En caso de cambio, se deberá reflejar la nueva realidad.

- Regular los intercambios de información con terceros formalmente, comunicando los requisitos al personal de la organización y a los terceros involucrados en dichos intercambios.

- Se definen las funciones y responsabilidades de todo el personal formalmente, y se establecen contratos y Cláusulas de Confidencialidad y Secreto profesional, en función de las responsabilidades y puestos asumidos en la organización. Se comunicarán a todos los empleados que como usuarios tengan acceso al Sistema de Información de la empresa, firmando los contratos como evidencia de la información recibida.
- Se establecen procesos formales de eliminación y reutilización de soportes que garanticen la confidencialidad de la información almacenada en ellos. La empresa decide definir las medidas de reutilización y desecho de los soportes de la empresa. Antes de cambiar de ubicación el equipo se procede a la eliminación de toda la información del disco duro del equipo. Para los disquetes y CD's desechados se establecen medidas de destrucción física antes de tirarlos a la papelera.

Con estas medidas se impide el acceso a los datos que contenían los soportes antes de su reutilización o desecho.

- Seleccionar un procedimiento de asignación de contraseñas así como concienciar y formar a los usuarios sobre la importancia de la confidencialidad de las mismas y sobre la elección de contraseñas robustas.
- Se restringe el uso de los servicios públicos (Internet) a aquellos usuarios autorizados expresamente para su uso. Los usuarios autorizados deberán conocer las posibles amenazas que pueden presentar, con un uso indebido del servicio. Por ello queda expresamente prohibido, descargarse cualquier aplicación o programa en equipos de la organización, que puedan dañar el Sistema de Información, sin la autorización expresa del Responsable de los Ficheros o Responsable de Tratamiento en la organización. La empresa decide definir que los usuarios externos solo podrán conectarse desde unos equipos determinados, que garantizan los niveles de seguridad exigidos por la empresa. De esta forma evita que se pueda acceder al sistema de información desde terminales que no sean de confianza.

- Se establecerán controles relacionados con el personal, incluyendo formación y concienciación, funciones, confidencialidad y recomendaciones a aplicar y controles relacionados con el sistema de información, incluyendo la seguridad física en el entorno y soportes, y la seguridad lógica en las comunicaciones.

- Se informa a todos los usuarios, que el uso del correo electrónico corporativo se utilizará para temas relacionados con la actividad laboral y que como medidas de seguridad, debemos tener presente: “No abrir correos sospechosos, de direcciones desconocidas o con asuntos poco fiables”, “no abrir ningún archivo adjunto sin antes analizarlo con un antivirus”, “no enviar información confidencial sin cifrado”.

# 6. RESPONSABLES DEL DESARROLLO, IMPLANTACIÓN Y GESTIÓN DE LA POLÍTICA DE SEGURIDAD

## 6.1. Responsable de Ficheros

Como representante de máxima autoridad de los Ficheros y del Sistema de Información de la empresa, deberá aprobar y publicar las medidas de seguridad establecidas en la organización, acorde con el cumplimiento de la LOPD.
Para ello establecerá controles relacionados con el negocio, tales como políticas de seguridad corporativas, relaciones con terceros, acuerdos de confidencialidad, etc., que se deben tener en cuenta de forma común por toda la organización.
Además de establecer un Plan de Continuidad de Negocio que garantice la recuperación de los sistemas en caso de desastre.

## 6.2. Responsable de tratamiento

Queda definida la figura del responsable de tratamiento en el apartado de "Glosario de Términos en el presente documento"

## 6.3. Responsable del Departamento de Informática

El responsable del Departamento de Informática en la organización o en su defecto la persona encargada de su mantenimiento, será la persona encargada de desarrollar e implantar todas las medidas de seguridad necesarias que afecten de manera directa al Sistema de Información de la empresa en Soporte informático. Para ello deberá:

- Definir un procedimiento de gestión de incidencias de seguridad y entregar a cada usuario sus obligaciones para el adecuado cumplimiento del mismo.
- Se debe establecer una política de copias de seguridad que garanticen la reconstrucción de los datos y configuración de los sistemas al instante anterior a la pérdida de información.
- Establecer procedimientos de mantenimiento de equipos y garantizar que son ejecutados por personal cualificado de forma periódica.
- Sincronizar los relojes de los servidores con arreglo a la norma UCT (Tiempo universal Coordinado). Implantación de Medidas Todos los relojes de los equipos del sistema de información se deberían sincronizar ajustado a la norma acordada UTC (Tiempo Universal Coordinado) y ajustado a la hora local normalizada. Este hecho permite la correcta realización de un análisis del rastro dejado por una evidencia en la secuencia de acciones cronológicamente correcta en el tiempo.

## 6.4. Usuarios del Sistema

Los usuarios del Sistema de Información de la empresa deberán cumplir con las normas expuestas en el presente documento así como las indicadas en los diferentes documentos que aparecen anexos al presente documento y que irían relacionados en función del perfil que adopten en la empresa.

## ANEXOS AL DOCUMENTO

- Modelo clausulas clientes
- Modelo clausula correos comerciales
- Modelo contrato confidencialidad proveedores
- Modelo contrato trabajadores
- Modelo responsabilidades trabajadores
- Documento de seguridad
- Guía para el uso de aplicaciones informáticas

**Avda. de Humanes, 155 – Nave 3.5**

Tel. +34 **918 106 925** – Fax: +34 **918 106 932**

28971 **Griñón** *Madrid*

**C/ El Pasadero, 6**

Tel y Fax: + 34 **987 794 330**

24416 **Santo Tomás de las Ollas** (Ponferrada) *León*

**Edificio Centris, planta -2, módulo 3**

Tel: +34 **955 312 665** – Fax: +34 **955 312 666**

41940 **Tomares** *Sevilla*