POLÍTICA DEL SGSI

FECHA	EDICIÓN	NATURALEZA DEL CAMBIO
30/06/2016	01	PRIMER EJEMPLAR

ÍNDICE

1. POLÍTICA DE SEGURIDAD

1.1. OBJETIVOS

Este documento tiene como objetivo establecer las directrices que garanticen, la disponibilidad, integridad y confidencialidad de la información en **TESLA TECHNOLOGIES, S.L.** (en adelante **TESLA**) a un nivel adecuado según el riesgo de los activos, las necesidades y los recursos. La política de seguridad de **TESLA** pretende:

- Asegurar que la plantilla conoce y comprende los problemas asociados a la seguridad de la información y que asumen y son conscientes de sus responsabilidades en este tema.
- Proporcionar una guía para establecer los estándares, procedimientos y medidas de seguridad para desarrollar un Sistema de Gestión de Seguridad de la Información.
- Asegurar la confidencialidad de la información que nuestros clientes depositan y **TESLA** almacena en los sistemas de información.
- Maximizar la disponibilidad y calidad de los servicios prestados a los clientes de **TESLA**.
- Reducir o eliminar las amenazas y riesgos inherentes a nuestras actividades por medio de la mejora continua del desempeño en seguridad en nuestros procesos, productos y servicios.
- Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información.
- Mantener a disposición de las partes interesadas la Política presente, así como los futuros desarrollos de la misma.

1.2. ALCANCE

El alcance del sistema de gestión de seguridad de la información abarca todos los sistemas de información que soportan los procesos de negocio de **TESLA**. Este alcance se encuentra desarrollado en términos de actividad empresarial, organización, ubicación, activos y tecnología, incluyendo la justificación de cualquier exclusión, según se indica a continuación:

Actividad empresarial

TESLA TECHNOLOGIES, es una entidad dedicada a ofrecer soluciones software a pequeñas y medianas empresas ligados al desarrollo de soluciones propias, en el ámbito Europeo y Norteamericano.

Dentro de estas soluciones propias, TESLA TECHNOLOGIES centra sus esfuerzos en la creación de una plataforma de comercio electrónico, que sea accesible a toda clase de clientes, promoviendo así el uso de tiendas Web en toda la sociedad.

Dentro del propósito de TESLA TECHNOLOGIES se encuentra el de fomentar la innovación y el empleo, generado riqueza en el ámbito tecnológico.

El domicilio social de TESLA TECHNOLOGIES se encuentra declarado en Rúa Fontiñas 92 en Santiago de Compostela, y dispone de una única sede situada en Rúa Pilar Miro 6 en Santiago de Compostela.

ESTRUCTURA DE LA ENTIDAD

TESLA TECHNOLOGIES esta formada por un equipo humano organizado en una estructura departamental por funciones, dando lugar a una jerarquía piramidal, donde la dirección esta en la cima de la pirámide, seguida de los diferentes responsables departamentales.

Estructura organizativa

La estrategia y objetivos de TESLA forman un valor corporativo enfocado al cliente que busca un equipo humano de calidad, con un alto nivel de conocimientos y especialización, capaz de generar y gestionar oportunidades de negocio con rigor y eficacia.

Para ello, TESLA ha desarrollado una política de Recursos Humanos basada en cuatro pilares básicos sobre los que se asienta nuestra cultura corporativa, que se resumen en:

- Captar, conservar y motivar a personas con talento.
- Actuar con rapidez, con capacidad para tomar decisiones, reduciendo al máximo la burocracia.
- Fomentar e incrementar la formación y el aprendizaje.
- Innovar, con ideas que permitan mejorar procesos, productos y servicios.

Todo ello ha sido posible gracias a un gran equipo humano plenamente identificado y comprometido con el proyecto estratégico de TESLA y a la aplicación de las políticas apropiadas en tres campos esenciales como son la incorporación de nuevo personal, la formación y desarrollo de la plantilla, y la prevención de riesgos laborales.

La estructura organizativa y funcional de TESLA se define en el siguiente organigrama, que proporciona la escalabilidad permitiendo manejar el crecimiento continuo de trabajo de manera fluida:

De forma semestral se reúne el Comité de Seguridad del SGSI, en el que se incluye: Un representante de la Dirección, el Responsable de Seguridad de la Información (RSI) y los administradores de sistema para la revisión del funcionamiento del SGSI. En dicha reunión se revisarán, como mínimo, las siguientes cuestiones:

- Seguimiento Objetivos del SGSI
- Revisión de las acciones planteadas en la Revisión por la dirección. Toma de acciones, si procede.
- Revisión del Plan de Tratamiento de Riesgos.
- Estado de acciones correctivas o preventivas, seguimiento.
- Resultados de los indicadores. Planificación de acciones, si procede.
- Estado de eficacia de los controles.
- Realización de las inspecciones. Análisis de Resultados y Planificación de acciones, si procede.
- Revisión de fichas de equipos informáticos sometidos a mantenimiento preventivo.
- Revisión registros LOPD (copias de seguridad, incidencias,..).
- Cambios que puedan afectar al SGSI.
- Conclusiones

De dichas reuniones, se dejará constancia mediante un acta en el que se reflejarán los puntos anteriores, acciones a cometer, plazos, recursos, y finalmente, se procederá a su revisión y aprobación por dirección. Dicha revisión se podrá realizar conjuntamente con la Revisión por la Dirección anual (punto 1.5 del presente documento).

Activos y tecnología

Los activos de información que **TESLA** dispone son los necesarios para la

prestación de su servicio y la gestión interna de la organización se pueden definir en los siguientes términos: servidores, ordenadores de sobremesa, portátiles, unidad de backup, bases de datos, sistema operativo, software y hardware.

Partes interesadas

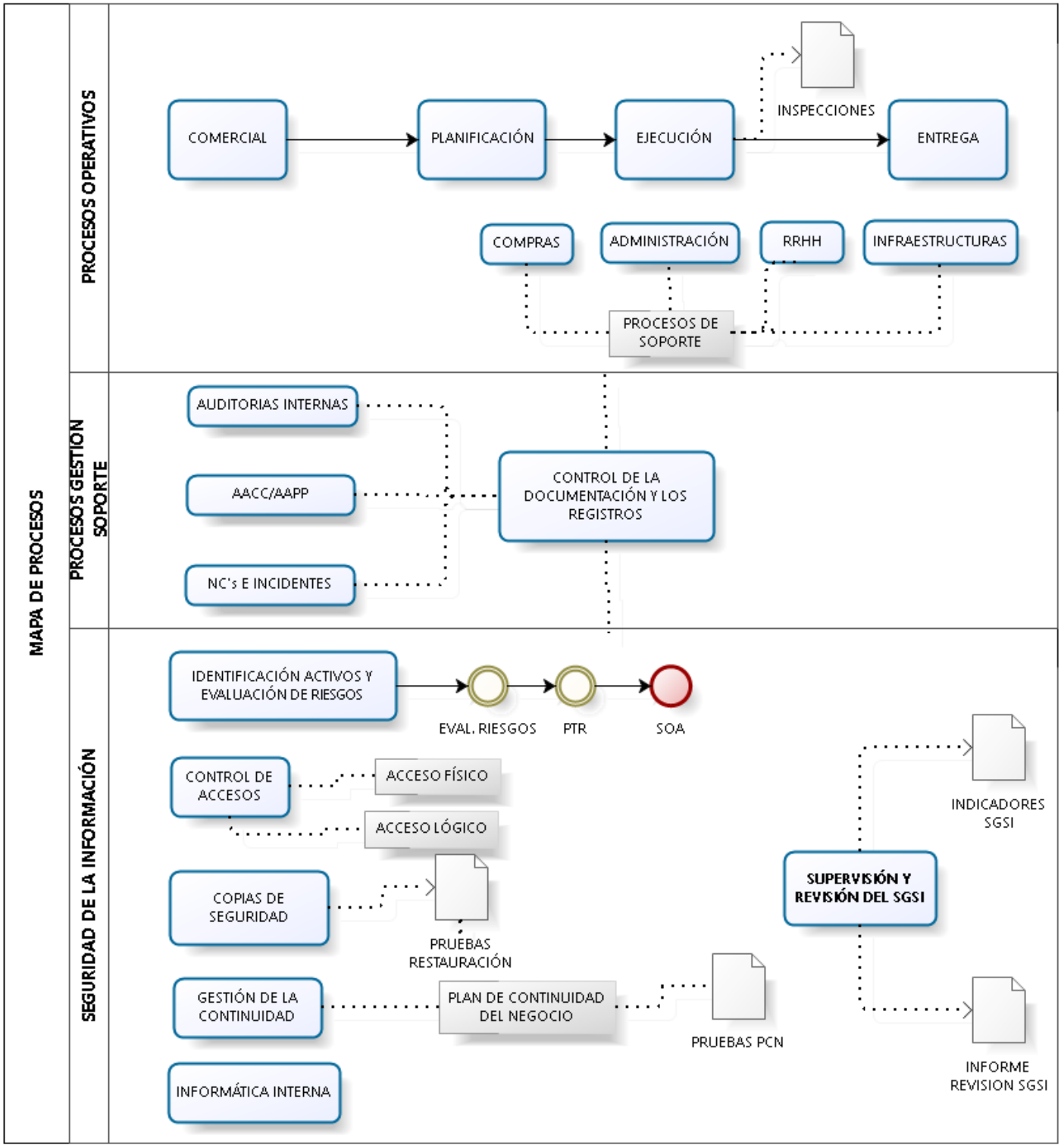
A continuación se identifican las partes interesadas, las cuestiones (tanto internas como externas) que afectan a **TESLA** para lograr los resultados previstos y los requisitos de las mismas en términos de seguridad de la información:

PARTE INTERESADA	CUESTIÓN	REQUISITOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN
SOCIOS (PARTNERS)	EXTERNA	Seguir las políticas de seguridad y de uso aceptable establecidas (si es el caso) por el partner.
PROVEEDORES	EXTERNA	Mantenimiento de la información de los proveedores de modo seguro. LOPD.
CLIENTES	EXTERNA	Certificación ISO 27001. Confidencialidad y seguridad de la información manejada. LOPD. Aplicar correctamente todas nuestras políticas de seguridad en el manejo de la información de los clientes.
EMPLEADOS	INTERNA	Nivel de seguridad alto manteniendo la operatividad en el trabajo diario.
DIRECCIÓN	INTERNA	Certificación ISO 27001.

Alcance del SGSI (Sistema de Gestión de Seguridad de la Información):

"Los sistemas de seguridad de la información que soportan los servicios de desarrollo de software relacionados con el diseño e implementación de páginas web en HTML5/CSS3, desarrollo de aplicaciones a medida en JAVA y PHP, comercio electrónico y formación relacionada con nuestros servicios y las tecnologías utilizadas por TESLA TECHNOLOGIES" de acuerdo al documento de Aplicabilidad vigente.

Los procesos del SGSI de **TESLA** se detallan en el modo de interrelacionar en el siguiente Mapa de Procesos, siendo los procesos de seguridad de la información y de gestión soporte los que afectan directamente al Sistema de Gestión de Seguridad de la Información:



1.3. PLANIFICACIÓN

Hay que tener en cuenta que no toda la información de la que dispone la organización tiene el mismo valor, e igualmente, no toda la información está sometida a los mismos riesgos. Por ello, periódicamente, se va a realizar una Evaluación de Riesgos que ofrezca una valoración de los activos de información y de las amenazas y vulnerabilidades a las que están expuestos. La Dirección de **TESLA** debe establecer anualmente unos Objetivos relacionados con la mejora del SGSI de modo que se busque la mejora continua a través del establecimiento de metas, plazos, responsables y recursos para la consecución de los mismos.

El resultado de la Gestión de Riesgos es el establecimiento de una serie de tareas a implantar, adecuadamente priorizadas, para mitigar los riesgos no asumibles. El proceso de Identificación de activos y evaluación de riesgos se detalla en el procedimiento P-04.

1.4. IMPLANTACIÓN

El Responsable de Seguridad de la Información (RSI) garantizará la implementación de los controles seleccionados, con una adecuada delimitación de responsabilidades y gestión de todo el personal involucrado, canalizando las directrices y normativas hacia las distintas líneas de negocio.

Actualmente en **TESLA** existe un RSI que se encargará de todas estas funciones y será el encargado de definir la estructura organizativa de seguridad.

1.5. REVISIÓN

El RSI revisará esta Política anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la Dirección.

El RSI será el encargado de realizar el adecuado control interno para evaluar la eficacia de los controles implementados en **TESLA** y tener actualizados todos los procedimientos y procesos aplicados en la empresa ante posibles cambios de negocio o de requisitos de seguridad.

Se realizará una auditoría interna anual que compruebe el nivel de cumplimiento del sistema de gestión respecto de la norma de referencia: UNE-ISO/IEC 27001. El proceso de auditorías internas se detalla en el procedimiento P-01.

Se realizará una revisión global del sistema, con periodicidad anual, en la que se valore la eficacia del sistema, se revise el cumplimiento de los objetivos fijados y se establezcan nuevos objetivos para el siguiente ciclo del sistema.

En esta revisión, como mínimo, se tratarán los siguientes puntos:

1. Revisión y adecuación de la Política del SGSI. Resultados obtenidos en relación con los Objetivos planificados en el documento "Objetivos del SGSI" para el período analizado.
2. Resultados de las auditorías internas y externas.
3. Estado de las no conformidades, acciones correctivas y preventivas.
4. Análisis de comentarios de los empleados y/o partes interesadas (clientes,

usuarios y proveedores).

5. Cambios que se hagan o tengan que producirse en la organización o actividades de **TESLA**, relacionadas con el SGSI.

6. Las técnicas, productos o procedimientos que podrían utilizarse dentro de la organización para mejorar el comportamiento y la eficacia del SGSI.

7. Revisión de vulnerabilidades o amenazas de seguridad de la información no abordadas adecuadamente en la evaluación de riesgos.

8. Resultados de las mediciones de la eficacia de los controles de seguridad de la información.

9. Resultados de las acciones de seguimiento de revisiones por la dirección previas.

10. Recomendaciones para la mejora.

En esta revisión, como mínimo, se analizarán los siguientes resultados:

a) La mejora de la eficacia del SGSI;

b) La actualización de la evaluación de riesgos y del plan de tratamiento de riesgos;

c) La modificación de los procedimientos y controles que afectan a la seguridad de la información, cuando sea necesario para responder a los eventos internos o externos que pueden afectar al SGSI, incluyendo los cambios en:

1. Los requisitos del negocio;
2. Los requisitos de seguridad;
3. Los procesos de negocio que afectan a los requisitos de negocio existentes;
4. Los requisitos legales o reglamentarios;
5. Las obligaciones contractuales; y
6. Los niveles de riesgo y/o los criterios de aceptación de los riesgos.
7. Las necesidades de recursos;
8. La mejora en el modo de medir la eficacia de los controles.

1.6. MEJORA

Para optimizar y mejorar de modo permanente el sistema de gestión de la seguridad de la información, se seguirán las reglas principales siguientes:

- El análisis periódico de las mejoras propuestas y toma de decisión durante la Revisión por la Dirección.
- El registro y seguimiento de las acciones correctivas y preventivas realizadas. Este proceso se detalla en el procedimiento P-02.

En cada ciclo del sistema se plantearán nuevos objetivos de mejora, planificándolos adecuadamente para poder realizar su correspondiente seguimiento.

2. RESPONSABILIDADES ASOCIADAS A LOS ACTIVOS

El RSI debe proporcionar ayuda y soporte a los propietarios de los activos de información para asegurar que se cumple la Política del SGSI y que la información y los sistemas están adecuadamente protegidos.

Para gestionar correctamente los activos el RSI mantendrá un inventario actualizado de los activos importantes donde quedará reflejado quién es el propietario del activo y donde está ubicado física o lógicamente el activo.

El propietario de un activo, entendiendo por tal al responsable de dicho activo, tendrá las siguientes responsabilidades:

- Valorar si el activo está afectado por la Ley de Protección de Datos y aplicarle en su caso, los procedimientos correspondientes.
- Asegurarse de que el software que se utiliza tiene licencia.
- Definir quiénes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación de la información y la función a desempeñar.
- Asegurarse de que el activo cuenta con el mantenimiento adecuado.
- Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del activo deberá informar a su vez al RSI para tratar la incidencia. La gestión de incidencias se describe en detalle en el procedimiento P-02.
- Asegurarse de que la plantilla cuenta con la formación adecuada, conoce y comprende la Política de Seguridad y pone en práctica las directrices de seguridad.
- Asegurarse de que los soportes y equipos que contengan información son desechados según lo establecido.
- Implementar las medidas de seguridad necesarias en su área para evitar fraudes, robos o interrupción en los servicios.
- Mantener documentación actualizada de todas las funciones críticas para asegurar la continuidad de las operaciones en caso de que alguien no esté disponible.
- Informar al RSI cuando ocurran cambios de personal que afecten al acceso de la información o los sistemas (cambio de función o departamento, causar baja en la empresa) para que se modifiquen apropiadamente los permisos de acceso.
- En los casos que aplique, asegurarse de que el personal y los contratistas tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

Todas estas funciones podrán ser delegadas en la figura del RSI.

2.1. EQUIPOS INFORMÁTICOS Y DE COMUNICACIONES Y SUS PROGRAMAS DE SOFTWARE

Para garantizar el correcto uso y operación de los equipos y los programas instalados, que se entregan al usuario debidamente configurados para su desempeño, se seguirán las reglas principales siguientes:

- Todos los equipos y sistemas son activos propiedad de **TESLA**, asignados a sus usuarios y puestos a su disposición exclusivamente para la realización de su trabajo.
- La instalación y uso de cualquier programa informático o contenido ajeno a los instalados o autorizados expresamente por **TESLA** queda terminantemente restringida. Asimismo, no se admiten modificaciones a los elementos del hardware entregado.
- Todos los programas informáticos instalados o embebidos en los equipos contarán con las debidas licencias de uso y/o mantenimiento emitidas por sus fabricantes.

2.2. PROTECCIÓN DEL CONOCIMIENTO

Para evitar la pérdida, robo o transferencia no autorizada de la propiedad intelectual o información clasificada por **TESLA**, se seguirán las reglas principales siguientes:

- La identificación y clasificación de toda la información, en cualquier soporte, considerada de especial protección.
- La firma por parte de todos los usuarios de un compromiso de confidencialidad.
- El seguimiento de todos los controles para el acceso, manejo, reproducción de dicha información.
- La monitorización de estos controles.
- El seguimiento de una política de puesto de trabajo despejado de papeles con información relevante y bloqueo de pantalla mediante contraseña cuando el equipo esté desatendido o no esté en uso, para asegurar la protección de información sensible.

2.3. PROPIETARIOS DE LA INFORMACIÓN

Todos los activos de información tendrán un Propietario, asignándole la responsabilidad del mantenimiento de los controles apropiados.

Para garantizar que se realiza una protección eficaz, el RSI impulsará la realización de un Inventario de Activos. Este proceso es un aspecto muy importante de la Gestión de Riesgos, ya que permite identificar el valor e importancia relativa a cada activo. Este inventario, se puede dividir según los activos asociados con los Sistemas de Información.

Los activos de información serán clasificados de acuerdo con la siguiente escala:

- **Confidencial:** Información a la que sólo determinadas personas o departamentos dentro de la organización deben tener acceso. Si se filtrara a terceras partes, podría tener consecuencias negativas para la organización
- **Uso Interno:** Información a la que sólo debe tener acceso el personal de la organización. Si se filtrara a terceras partes, podría tener consecuencias para la organización.
- **Público:** Información sin ninguna restricción de acceso. Si se filtrara a

terceras partes, no tendría consecuencias para la organización

La información confidencial será marcada como tal. Tanto la autorización de acceso como la transmisión de esta información por cualquier medio necesitan la aprobación expresa del responsable del activo. La destrucción de esta información la realizará el responsable del activo siguiendo las pautas aprobadas por el RSI y con su colaboración si es necesaria.

3. SEGURIDAD DE LA GESTIÓN DE RECURSOS HUMANOS

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Se realizarán comprobaciones previas a la contratación de nuevos empleados como por ejemplo:

- Referencias personales.
- Comprobación del Currículo Vital.
- Confirmación de certificaciones académicas.

A los empleados de **TESLA** se les requerirá la firma de un acuerdo de confidencialidad para evitar la divulgación de información secreta. Así mismo, cuando se termine la relación laboral o contractual, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede y aquellos que infrinjan las normas de Seguridad pueden ser sancionados.

En las condiciones de la relación laboral deberán quedar reflejadas las responsabilidades del empleado en materia de seguridad de la información. Esta responsabilidad continuará tras la finalización del contrato.

La gestión de RRHH se detalla en el procedimiento P-06 "Gestión de RRHH" y la instrucción IS01-P-06 "Funciones y obligaciones de usuarios de la información".

4. SEGURIDAD FÍSICA Y DEL ENTORNO

Para que una seguridad lógica sea efectiva es primordial que las instalaciones de **TESLA** mantengan una correcta seguridad física para evitar los accesos no autorizados, así como, cualquier otro tipo de daño o interferencia externa. **TESLA** tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.

La totalidad de las oficinas de **TESLA** cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen. Las salas donde se ubican los sistemas y el cableado permanecerán cerradas y sólo tendrán acceso las personas autorizadas y los terceros cuando vayan acompañados por alguien autorizado.

Las instalaciones están dotadas de dispositivos de extinción de incendios marcados por la legislación vigente en esa materia. En este sentido, se dispone de extintores y salidas de emergencia debidamente señalizados.

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado, de forma que mantengan la confidencialidad, integridad y la disponibilidad de la información. Para ello, deben someterse a las revisiones recomendadas por el suministrador. Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación.

La eliminación de equipos sólo se llevará a cabo por el RSI o personal en el que éste delegue.

5. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Para la seguridad relativa a comunicaciones, soportes, redes de datos, código malicioso y copias de seguridad, se adjuntan las siguientes instrucciones de seguridad:

a) IS03-PSI-01 "Tratamiento, Protección y Eliminación de Datos en Soportes y Dispositivos Móviles".
b) IS04-PSI-01 "Uso de Internet, Navegadores, Hosting y Acceso a la Información".
c) IS05-PSI-01 "Uso del Correo Electrónico, Mensajería, Voz y Difusión de la Información".
d) IS06-PSI-01 "Detección y Tratamiento de Malware".
e) IS07-PSI-01 "Realización, verificación y restauración de copias de seguridad".
f) IS08-PSI-01 "Monitorización, supervisión y control de la información y las comunicaciones".

Adicionalmente a lo expuesto en dichas instrucciones, se añaden los siguientes elementos y sus ámbitos correspondientes:

5.1. Filtrado de contenidos

Para garantizar la identificación, el bloqueo y eliminación de contenidos potencialmente maliciosos, **TESLA** mantiene un sistema antivirus en todos los equipos.

5.2. Correo electrónico

Para garantizar el debido uso del correo electrónico por parte de los usuarios, se seguirán las reglas principales siguientes:

- Las cuentas de correo electrónico asignadas a los usuarios para el desempeño de sus actividades profesionales, son propiedad de **TESLA**.
- Los contenidos de los correos electrónicos son confidenciales ajustándose al ordenamiento legal.
- A todos los usuarios de las cuentas de correo electrónico se le asigna una dirección electrónica y una contraseña, que serán estrictamente personales e intransferibles.
- La contraseña será configurada por el usuario de acuerdo con las instrucciones dadas por **TESLA**.
- Como reglas generales se recomienda:
  - No abrir nunca o reenviar mensajes de correo de remitentes desconocidos.

- No abrir nunca o reenviar mensajes de correo de remitentes conocidos pero con asuntos en idiomas diferentes de su remitente.
- No abrir nunca los ficheros adjuntos de correos de procedencia dudosa.

5.3. Intercambio de Información

Cuando se realice intercambio de información de carácter confidencial, tanto interna como externamente, se protegerá mediante cifrado AES256.

6. CONTROL DE ACCESOS

6.1. Identificación y autentificación de los usuarios

La información debe estar protegida contra accesos no autorizados, por ello, cada responsable de departamento o área definirá las necesidades de acceso a la información y sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

Para garantizar el debido acceso a los equipos, programas informáticos y datos, se seguirán las reglas principales siguientes:

- A todo usuario de los sistemas se le asigna un nombre de usuario y una contraseña, que serán estrictamente personales e intransferibles.
- Cada perfil de usuario dispondrá de unos determinados permisos.
- La contraseña será configurada por el usuario de acuerdo con las instrucciones dadas por **TESLA**.
- Las contraseñas deberán renovarse periódicamente.

La gestión de Control de Accesos se detalla en las instrucciones IS01-PSI-01 "Control de acceso físico y protección de la instalación" y IS02-PSI-01 "Usuarios, identificadores y contraseñas".

6.2. Acceso a Internet

No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

El RSI controlará las altas, modificaciones y bajas de todos los usuarios.

7. ADQUISICIÓN, DESARROLLO Y MATENIMIENTO DE SISTEMAS

Para afrontar y delimitar las acciones de control relacionadas con los sistemas de información, su modificación, desarrollo, actualización o adquisición se adjuntan las siguientes instrucciones de seguridad:

- IS13-PSI-01 Actualización de Sistemas y Equipamiento.
- IS08-PSI-01 Control, supervisión y planificación de actividades o modificaciones de equipamiento TI
- IS11-PSI-01 Tratamiento de datos y código fuente en desarrollo de aplicaciones

8. GESTIÓN DE INCIDENCIAS

Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al RSI para que tome las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

La gestión de Incidencias se detalla en el procedimiento P-02.

9. CONTINUIDAD DEL NEGOCIO

Es imprescindible para **TESLA** establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades del negocio por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad del negocio en estos casos, **TESLA** establecerá un plan de contingencia que permita la recuperación de las actividades al menos en un nivel mínimo, en un plazo razonable de tiempo. La gestión de la continuidad del negocio incluirá, por tanto, un procedimiento que limite las consecuencias dañinas de los desastres y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del negocio se documentará, partiendo de los riesgos detectados y de los controles existentes, que deberán probarse y actualizarse regularmente para comprobar su idoneidad.

La gestión de la continuidad de negocio se detalla en el procedimiento P-05.

10. Cumplimiento legal

El diseño, operación, uso y administración de los sistemas de información debe estar sujeto a requisitos de seguridad legal, normativa y contractual. Se deben impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, normas, reglamentos o contratos; y de los requisitos de seguridad.

- **TESLA** adquiere el compromiso de velar por el cumplimiento de la legislación vigente en materia de protección y seguridad de los Sistemas de Información, aplicable a todos sus procesos de negocio.
- **TESLA**, sus empleados y colaboradores se comprometen al uso y tratamiento de los datos personales adoptando las precauciones necesarias para garantizar el nivel de seguridad exigido por el marco legal vigente en materia de Protección de Datos de Carácter Personal.
- Los usuarios finales deben cumplir todas sus obligaciones considerando en todo momento las directrices marcadas por **TESLA** con el fin de no incumplir la legislación, informando a los responsables a través de las vías reglamentarias.

Con el fin de conseguir la conformidad de los sistemas con las políticas y

procedimientos de seguridad, se realizarán revisiones regulares de los sistemas.

Con respecto a la legislación vigente de protección de datos personales, se regirá por las referencias específicas a datos de carácter personal recogidas en las instrucciones de seguridad pertenecientes a éste procedimiento o P-05 "Gestión de Recursos Humanos", a las medidas, criterios, cláusulas y ficheros recogidos en el "Documento de Seguridad" y a los siguientes formatos específicos adjuntos:

- F01-PSI-01 "Inventario de Soportes".
- F02-PSI-01 "Autorización Alta-Baja Soportes".
- F03-PSI-01 "Registro Entrada/Salida de Soportes".
- F04-PSI-01 "Relación de Usuarios con Acceso Autorizado".

Con respecto a la legislación relativa a propiedad intelectual e industrial se procederá a analizar por el Responsable del SGSI la adecuación de las licencias y acuerdos relacionados con la cesión de derechos de propiedad intelectual relacionados con software y aplicaciones, patentes o marcas y en general a cualquier ámbito relacionado con propiedad intelectual y/o industrial.

Para llevar un registro de las licencias en posesión de **TESLA TECHNOLOGIES**, se generarán los registros necesarios con las licencias de software y similar material en el siguiente formato:

- F04-PSI-01 "Inventario de Licencias", adjuntando, si el Responsable del SGSI así lo estimase, lo documentos, contratos, facturas o evidencias que fundamenten los requisitos legales y condiciones de la cesión u otorgación de la licencia de uso, o análogas.

En lo relativo a la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico, **TESLA TECHNOLOGIES** cumple con los requisitos mínimos establecidos referentes a la información general e identificación a través de la Web corporativa, no existiendo a fecha de edición del presente procedimiento ninguna otra obligación, por la ausencia de actividades de comercio electrónico realizadas a través de la Web **www.teslatechnologies.es.**

Para delimitar el ámbito, uso y limitaciones de los certificados basados en la ley de Firma Electrónica, se atenderá a lo expuesto en IS04-PSI-01 "Uso de Internet, Navegadores, Hosting y Acceso a la Información".

Siendo el cumplimiento legal un requisito crítico para el correcto desempeño de la seguridad de la información desde múltiples perspectivas, cualquier desviación o incumplimiento relacionado con lo expuesto en este apartado será motivo suficiente para generar de inmediato una incidencia, recogida en el "Parte de Incidencias, No Conformidades, Acciones Correctivas y Preventivas", considerándose la implementación y puesta en marcha de la acciones correctivas encaminadas a subsanar dicha incidencia con la mayor urgencia y prioridad posibles.

Toda la legislación vinculante para la seguridad de la información se indica y referencia según lo establecido en el procedimiento P-03 Control de la documentación y los

registros.