POLÍTICA DE SEGURIDAD DEL ESQUEMA NACIONAL DE SEGURIDAD POL.01

REGISTRO DE EDICIONES

EDICIÓN	FECHA	RAZÓN DEL CAMBIO
00	29/10/2025	Edición inicial

	PREPARADO	REVISADO Y APROBADO
NOMBRE	Francisco Javier Cuenca García	José Manuel Martínez García
CARGO	Responsable Sistemas, Infraestructura y Seguridad	Director General
FECHA Y FIRMA (1)	Fecha: 29/10/2025	Fecha: 29/10/2025

(1) Por motivos de protección de datos de carácter personal esta versión del documento no muestra las firmas

INDICE

1 APROBACIÓN Y ENTRADA EN VIGOR. 3
2 ALCANCE....3
3 MISIÓN. 3
4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN....3
4.1 Revisión y aprobación.... 3
4.2 Desarrollo. 3
5 MARCO NORMATIVO. 3
6 GESTIÓN DE LA INFORMACIÓN DOCUMENTADA. 4
6.1 DOCUMENTACIÓN DEL SISTEMA. 4
7 PRINCIPIOS BÁSICOS DE SEGURIDAD. 4
7.1 SEGURIDAD INTEGRAL.... 4
7.2 GESTIÓN DE RIESGOS. 4
7.3 PREVENCIÓN, REACCIÓN Y RECUPERACIÓN. 4
7.3.1 Prevención.... 4
7.3.2 Respuesta. 5
7.3.3 Recuperación. 5
7.3.4 Conservación.... 5
7.4 LÍNEAS DE DEFENSA. 5
7.5 VIGILANCIA CONTINUA. 5
7.6 REEVALUACIÓN PERIÓDICA. 5
7.7 FUNCIÓN DIFERENCIADA.... 5
8 REQUISITOS MÍNIMOS DE SEGURIDAD....5
8.1 ORGANIZACIÓN DE LA SEGURIDAD.... 5
8.1.1 Roles: funciones y responsabilidades.... 5
8.1.2 Procedimientos de designación.... 8
8.1.3 Coordinación y Resolución de conflictos. 8
8.2 GESTIÓN DE RIESGOS. 8
8.3 GESTIÓN DEL PERSONAL. 8
8.4 PROFESIONALIDAD.... 8
8.5 AUTORIZACIÓN Y CONTROL DE LOS ACCESOS. 9
8.6 PROTECCIÓN DE LAS INSTALACIONES.... 9
8.7 ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD.... 9
8.8 SEGURIDAD POR DEFECTO.... 9
8.9 INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA. 9
8.10 PROTECCIÓN DE INFORMACIÓN ALMACENADA Y EN TRÁNSITO..... 9
8.11 PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS. 10
8.12 REGISTRO DE ACTIVIDAD.....10
8.13 INCIDENTES DE SEGURIDAD.....10
8.14 CONTINUIDAD DE LA ACTIVIDAD.....10
8.15 MEJORA CONTINUA DEL PROCESO DE SEGURIDAD. 10
9 DATOS DE CARÁCTER PERSONAL. 10
10 OBLIGACIONES DEL PERSONAL. 10
11 TERCERAS PARTES. 11
12 REGISTROS Y DOCUMENTACIÓN DE REFERENCIA....11

1 APROBACIÓN Y ENTRADA EN VIGOR.

Esta Política de Seguridad de la Información es efectiva desde su aprobación por el Comité de Seguridad y permanecerá vigente hasta que se realicen cambios o se anule.
La Política de Seguridad de la Información (en adelante PSI) se aplicará por todos los órganos superiores y directivos, a todos los sistemas de información que gestionen en el ejercicio de sus competencias, debiendo ser cumplida por su personal y por cualquiera que tenga acceso a sus sistemas de información.

2 ALCANCE.

El Alcance es la Gestión de Seguridad de la Información asociada a los “Los sistemas de información que sustentan los servicios para:

- Diseño, ejecución, puesta en marcha y mantenimiento de instalaciones eléctricas y mecánicas, incluidas instalaciones de energías renovables y sistemas de evacuación de la energía.
- Gestión y mantenimiento integral de elementos constructivos e instalaciones de edificios, recintos y oficinas dentro del sector público, industrial y terciario.
- Gestión y mantenimiento de equipos sanitarios para uso electromédico.

3 MISIÓN.

EIFFAGE ENERGIA es una empresa que presta servicios de soporte IT a organismos de las administraciones públicas y privada en el ámbito tecnológico.

4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Para mantener en todo momento la seguridad de nuestra información, nuestros sistemas y servicios, se ha desarrollado esta Política.
Para cumplir con lo requerido por el ENS, esta Política:

- Contempla los principios básicos y los requisitos mínimos
- Se aplica a los sistemas de información y activos utilizados para la prestación de nuestros servicios dentro del alcance.
- Es de obligado cumplimiento por todo el personal con acceso a los sistemas de información

4.1 Revisión y aprobación.

La Política se revisará al menos anualmente por el Comité de Seguridad.
Está aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

4.2 Desarrollo.

Esta Política está desarrollada por medio de nuestra NSI-00-Ed01-Norma_para_uso_de_SI.
Esta Normativa está 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.

5 MARCO NORMATIVO.

El marco normativo de las actividades bajo esta Política está integrado por todas las normas vigentes que afecten a la seguridad de la información en el ámbito de actuación de la Compañía.
Las acciones que la Compañía emprenda en materia de seguridad de la información serán acordes con las mejores prácticas de seguridad, recogidas en las guías del CCN-STIC del Centro Criptológico Nacional y otras normas internacionalmente reconocidas.
La legislación, normativa y guías en materia de seguridad de la información se recoge en el registro de documentación en vigor.

6 GESTIÓN DE LA INFORMACIÓN DOCUMENTADA.

6.1 DOCUMENTACIÓN DEL SISTEMA.

Cuando se genere documentación, en los casos en los que proceda, deben ser sometidos a revisión y una vez superada esta, deben remitirse al responsable de su aprobación para la misma, según la siguiente tabla.

DOCUMENTO	EMISIÓN	REVISIÓN	APROBACIÓN
Manual /Procedimientos	Responsable del Sistema	Comité de Gestión	Dirección
Instrucciones Técnicas/Registros	Responsable de la actividad	Jefe del Departamento	-

La revisión y aprobación de un documento no exige una reunión formal del Comité de Gestión, pudiendo sustituirse esta por la circulación del borrador del documento entre los miembros del Comité.
El Responsable del Sistema es la única persona autorizada para efectuar físicamente las modificaciones aprobadas sobre la documentación original del Sistema. Las modificaciones realizadas con respecto a la edición anterior se reflejan el apartado de Historial de Cambios indicando:

- Nueva versión
- Fecha
- Naturaleza de la revisión, en este apartado se incluye un resumen de los cambios y los apartados a los que afectan.

Finalizada la revisión el Responsable del Sistema retirará los documentos obsoletos sustituyéndolos por los revisados, poniéndolos a disposición del personal que será notificado de los cambios.
Estas modificaciones quedarán reflejadas en la Lista de Documentación en Vigor.
Los documentos obsoletos serán conservados por un período de 3 años, salvo que exista algún requerimiento que nos obligue a conservarlo durante un periodo diferente, en cuyo caso se especificará en el Listado de documentación en vigor.

7 PRINCIPIOS BÁSICOS DE SEGURIDAD.

7.1 SEGURIDAD INTEGRAL.

Entendemos la seguridad como un proceso integral y así está planteado nuestro Sistema de Gestión de Seguridad de la Información, que comprende todos aspectos técnicos, humanos y organizativos para que las distintas medidas que se tomen funcionen coherentemente.
En este sentido, se trabaja en concienciación y formación para que todos los usuarios de nuestros sistemas tengan sensibilidad sobre los riesgos que se corren, las medidas que se han implantado para mitigarlos y su responsabilidad en el éxito de la implantación de estas medidas.

7.2 GESTIÓN DE RIESGOS.

Se han definido las pautas para la gestión de los riesgos en el procedimiento correspondiente.

7.3 PREVENCIÓN, REACCIÓN Y RECUPERACIÓN.

7.3.1 Prevención.

Se cuenta con medidas para 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 implementamos las medidas mínimas de seguridad determinadas en el marco normativo definido, así como cualquier control adicional identificado a través de la evaluación de amenazas y riesgos.
Estos controles, y los roles y responsabilidades de seguridad de todo el personal, están definidos y documentados.

Como parte de esta prevención:

- Se monitoriza la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.
- 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.
- La entrada en operación de nuevos sistemas requiere autorización
- Se evalúa periódicamente la seguridad, incluso por terceros.

7.3.2 Respuesta.

Hay establecidos mecanismos para responder eficazmente a los incidentes de seguridad, con un punto de contacto para comunicar eventos e incidentes y protocolos de actuación.

7.3.3 Recuperación.

Para garantizar la disponibilidad de los servicios críticos, se han desarrollado planes de contingencia de los sistemas TIC como parte del plan general de continuidad del negocio y actividades de recuperación.

7.3.4 Conservación.

Nuestro sistema de contingencia garantiza la conservación de los datos y la información en soporte electrónico. El Sistema de Gestión de Seguridad de la información implementado mantiene disponibles los mismos durante todo su ciclo de vida.

7.4 LÍNEAS DE DEFENSA.

Nuestra estrategia de seguridad cuenta con líneas de defensa que nos permiten reaccionar adecuadamente a los incidentes que inevitablemente ocurran, ganando tiempo en la medida de lo posible, reduciendo la probabilidad de un fallo total y el impacto final del incidente.

7.5 VIGILANCIA CONTINUA.

Se cuenta con un sistema de vigilancia continua que permite detectar actividades anómalas para dar así una rápida respuesta.
Estas medidas se revisan y actualizan periódicamente.

7.6 REEVALUACIÓN PERIÓDICA.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

7.7 FUNCIÓN DIFERENCIADA.

Hay distintas funciones que estarán diferenciadas para evitar conflictos de interés:

- En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.
- La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

8 REQUISITOS MÍNIMOS DE SEGURIDAD.

8.1 ORGANIZACIÓN DE LA SEGURIDAD.

8.1.1 Roles: funciones y responsabilidades.

Rol	Funciones
Dirección General	Su titular ostenta la máxima responsabilidad en el desarrollo de las competencias de la entidad, incluyendo las de seguridad de la información. Es el máximo responsable de la implantación del ENS.
Comité de Seguridad de la Información	Estará formado por la dirección general y los responsables del servicio, información, seguridad y sistema, convocándose a responsables de área según se necesite. Se encargará de: • Informar regularmente del estado de la seguridad de la información a la Dirección • Elaborar la estrategia y promover la mejora continua de la gestión de la seguridad de la información. • Gestionar la elaboración y la aprobación de la documentación necesaria. • Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades. • Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados. • Supervisará el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, coordinará todas las actividades relacionadas con la seguridad de la información. • Impulsar el cumplimiento de la PSI y su desarrollo normativo. • Velar por el cumplimiento y difusión de la PSI, promoviendo actividades de concienciación y formación en materia de seguridad para el personal del Departamento. • Tomar aquellas decisiones que garanticen la seguridad de la información y de los servicios del Departamento. El Comité se reunirá con carácter ordinario, al menos, anualmente. Por razones de urgencia podrá reunirse siempre que el Director General lo estime conveniente.
Responsable de la Información	Determinará los requisitos de seguridad de la información tratada establecidos en el Real Decreto 311/2022, de 3 de mayo, y la función será asumida por la Dirección General. Sus funciones principales son: • Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes de seguridad. • Son los encargados, junto a los Responsables del Servicio y contando con la participación del Responsable de la Seguridad, de realizar los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar. • Aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos. Para la determinación de los niveles de seguridad de la información, el Responsable de la Información solicitará informe del Responsable de la Seguridad.
Responsable de Servicio	Responsable del servicio, determinará los requisitos de los servicios prestados establecidos en el Real Decreto 311/2022, de 3 de mayo, y la asume por la Dirección General. Sus funciones principales son:

	• Determinar los niveles de seguridad del servicio, valorando los impactos de los incidentes de seguridad. • Son los encargados, junto a los Responsables de la Información y contando con la participación del responsable de la seguridad, de realizar los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar. • Aceptar los riesgos residuales respecto de los servicios calculados en el análisis de riesgos. Para la determinación de los niveles de seguridad del servicio, el Responsable del Servicio solicitará informe del Responsable de la Seguridad.
El Responsable de la Seguridad.	Es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, asumiendo la función el Director de Productos. Sus funciones principales son: • Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización. • Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. • Velar por la ejecución de las decisiones del Comité. • Preparar los temas a tratar en las reuniones del Comité, realizar la convocatoria y elaborar el acta de las mismas; así como asesorar y darle soporte en cuantos asuntos estime de interés. • Verificar que las medidas de seguridad son adecuadas para la protección de la información y de los servicios. • Supervisar los sistemas de control interno, las evaluaciones periódicas de riesgos que se lleven a cabo y planificar las auditorías periódicas. • Promover la concienciación, educación y formación en materia de seguridad de la información a todo el personal. • Coordinar la investigación de incidentes de seguridad de la información. • Asumir las funciones explícitamente atribuidas a la figura del Responsable de Seguridad en el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en el Real Decreto 311/2022, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.
Responsable del Sistema.	El Responsable del Sistema es la persona que tiene la responsabilidad de desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento, asumiendo la función el Responsable de SGI. Sus funciones principales son: • 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 de seguridad se integren adecuadamente en el marco general de seguridad.
Responsable de Protección de Datos	El Responsable de Protección de Datos es la persona que atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas la legislación vigente.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la PSI prevalecerá la decisión del Comité de Seguridad de la Información.

8.1.2 Procedimientos de designación.

Los cargos serán nombrados por la Dirección a propuesta del Comité de Seguridad, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

8.1.3 Coordinación y Resolución de conflictos.

La coordinación de los responsables recae en la dirección y en caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos.
En defecto de lo anterior, prevalecerá la decisión del Director General.

8.2 GESTIÓN DE RIESGOS.

Todos los sistemas sujetos a esta Política se someten a un análisis de riesgos periódico, evaluando las amenazas y los riesgos a los que están expuestos realizado:

- 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

La valoración y tratamiento del riesgo se realiza según lo descrito en el procedimiento de Gestión de riesgos.

La valoración del riesgo queda recogida en el Análisis de Riesgos.

Los controles seleccionados para reducir los riesgos se detallan en el Documento de Aplicabilidad.

Las acciones para tratar el riesgo se recogen en el Plan de Tratamiento del Riesgo.

La aprobación del riesgo residual y el Plan de Gestión se realizan en el marco del Comité de Seguridad, quedando documentadas en las actas de reunión.

8.3 GESTIÓN DEL PERSONAL.

Todo el personal relacionado con la información y los sistemas debe ser formado e informado de sus deberes y obligaciones en materia de seguridad. Se supervisan las actuaciones para verificar que se siguen los procedimientos establecidos.

El personal relacionado con la información y los sistemas ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

El significado y alcance del uso seguro del sistema se ha concretado y documentado en la Normativa de Seguridad y los procedimientos asociados.

Los usuarios de los sistemas se identifican de manera unívoca para gestionar correctamente los derechos de acceso y controlar el uso de estos derechos.

8.4 PROFESIONALIDAD.

La seguridad de los sistemas está atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

El personal recibe la formación específica necesaria para garantizar la seguridad de las tecnologías de la información en uso en la organización.

Los subcontratistas son cuidadosamente seleccionados y se les informa y forma para que presten sus servicios de acuerdo a nuestros niveles de profesionalidad y seguridad.

8.5 AUTORIZACIÓN Y CONTROL DE LOS ACCESOS.

Los accesos a los sistemas de información están controlados y limitados a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

8.6 PROTECCIÓN DE LAS INSTALACIONES.

El acceso a las instalaciones se encuentra restringido y controlado por controles de acceso. Los sistemas se ubican en salas con acceso restringido y controlado.

8.7 ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD.

Cuando se presten servicios a clientes o se ceda información a terceros se les hará partícipes de la presente Política de Seguridad de la Información y de las normas de seguridad o procedimientos de seguridad relacionados con el servicio o la información afectados.

Se establecerán canales de información y coordinación entre los respectivos responsables de gestión de la seguridad de la información y se establecerán procedimientos de seguridad para la reacción ante incidentes.

En los contratos de adquisición de sistemas o aplicaciones informáticas, de prestación de servicios tecnológicos, y también en el caso de contratos de prestación de servicios de otro tipo que implique el uso de servicios, aplicaciones o sistemas informáticos internos, se considerarán los requisitos y medidas de seguridad aplicables.

Siempre que sea posible y a juicio del Responsable de Seguridad se priorizará a aquellos proveedores que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

8.8 SEGURIDAD POR DEFECTO.

Los sistemas se han diseñado y configurado de forma que garanticen la seguridad por defecto:

- Los sistemas proporcionan la mínima funcionalidad que cada usuario necesita para la ejecución de sus tareas, asegurando que su uso sea sencillo y seguro.
- Las funciones de operación, administración y registro de actividad son las mínimas necesarias, y sólo son accesibles por personal autorizado y desde emplazamientos o equipos autorizados.
- En los sistemas en producción se eliminan o desactivan, mediante el control de la configuración, las funciones que no son de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

8.9 INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA.

La instalación de cualquier elemento físico o lógico sigue un procedimiento formal con distintos niveles de autorización hasta su puesta en producción.

Se hace un seguimiento riguroso del estado de seguridad de los sistemas y se atiende a las recomendaciones y especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que afecten a los elementos de los sistemas, para impedir o mitigar los riesgos que vayan apareciendo.

8.10 PROTECCIÓN DE INFORMACIÓN ALMACENADA Y EN TRÁNSITO.

Somos rigurosos con la seguridad de la información almacenada en nuestros sistemas, así como la de la que se encuentra en tránsito. Para ello se ha diseñado e implantado las medidas técnicas y organizativas que se recogen en nuestro SGSI para proteger la información en cualquier punto o soporte en el que se encuentre.

8.11 PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS.

El perímetro en el que se ubican nuestros sistemas se encuentra debidamente protegido, así como los puntos de interconexión con redes ajenas.

8.12 REGISTRO DE ACTIVIDAD.

Con el fin de preservar la seguridad de nuestros sistemas, se recogen datos sobre la actividad de los usuarios con plenas garantías legales y de acuerdo con la normativa sobre protección de datos personales. Estos datos serán únicamente los necesarios para monitorizar, detectar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

8.13 INCIDENTES DE SEGURIDAD.

Nuestros sistemas de información cuentan con un sistema de detección y reacción frente a código dañino.

Estos y cualquier otro tipo de incidentes de seguridad se gestionan con las herramientas y procedimientos implantados al efecto, quedando registro de los mismos y de las actuaciones realizadas para resolverlos, Esta información se utiliza para evitar futuros incidentes, resolver antes lo que no se pueda evitar y tomar acciones de mejora.

8.14 CONTINUIDAD DE LA ACTIVIDAD.

Los sistemas disponen de copias de seguridad y se han establecido los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

8.15 MEJORA CONTINUA DEL PROCESO DE SEGURIDAD.

El proceso integral de seguridad implantado se actualiza y mejora en el marco de las normas que le aplican.

9 DATOS DE CARÁCTER PERSONAL.

EIFFAGE trata los datos de carácter personal según lo descrito en nuestro Documento de Seguridad, que recoge los tratamientos que se realizan y los responsables correspondientes. Todos los sistemas de información están protegidos en base a los requisitos definidos en la normativa de Protección de Datos, así como con las medidas aplicadas para reducir los riesgos identificados.

El Documento de Seguridad de Protección de Datos y la documentación relacionada están ubicados en el repositorio documental de la empresa.

Se ha nombrado un DPD para apoyar la correcta ejecución de nuestras obligaciones en este aspecto.

10 OBLIGACIONES DEL PERSONAL.

Todos los empleados de EIFFAGE tienen la obligación de conocer y cumplir esta Política de seguridad de la Información y la Normativa de Seguridad, el incumplimiento de esta obligación será sometido a las sanciones establecidas en nuestro convenio. Es responsabilidad de la Dirección disponer los medios necesarios para que la información llegue a los afectados.

Todos los empleados recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los empleados de EIFFAGE en particular a los de nueva incorporación.

EIFFAGE desarrolla actividades formativas específicas orientadas a la concienciación y formación de los empleados del Departamento, así como a la difusión entre los mismos de la PSI y de su desarrollo normativo. A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los Planes de Formación de EIFFAGE

11 TERCERAS PARTES.

Cuando prestamos servicios a otras organizaciones o manejamos información de otros, se les hace partícipes de esta Política de Seguridad de la Información, estableciendo canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando nosotros utilizamos servicios de terceros o cedemos información a terceros, se les hace partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña 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.

12 REGISTROS Y DOCUMENTACIÓN DE REFERENCIA

Los documentos de referencia son:

- Esquema Nacional de Seguridad
- MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
- Norma UNE-ISO 31000 Gestión del riesgo — Directrices
- Norma UNE-ISO/IEC 27001
- Norma UNE-ISO/IEC 27002

Los registros son:

- Listado de documentación en vigor
- Cuadro de mando
- Programa de auditorías
- Plan de auditoría
- Informe de auditoría interna
- Revisión por la dirección
- Acción de Mejora
- Acta de reunión
- Registros de formación.