PO27.01 Política Corporativa

Seguridad de la Información

Año: 2020

V.1.0

POLÍTICA

PÚBLICO

Normas de uso, acceso y distribución de este documento	
Queda prohibido cualquier tipo de explotación y, en particular, la reproducción, distribución, comunicación pública y/o transformación, total o parcial, por cualquier medio, de este documento sin el previo consentimiento expreso y por escrito de Seidor. Cualquier copia de este documento será considerada una copia no controlada y es responsabilidad del poseedor de dicha copia de verificar su vigencia	
Servicio responsable de este documento: Comité Corporativo de Ciberseguridad	
Seidor S.A Eix Once de Setembre núm.41 VIC CP.08500	Oficina de Ciberseguridad Corporativa Telf.902995374 c/e: occ@seidor.es

CONTENIDO

1 INTRODUCCIÓN

La información es un activo estratégico para para las empresas que conforman Grupo SEIDOR (en adelante **SEIDOR)**, como empresas cuya actividad principal se enmarca en la prestación de servicios de Tecnologías de la Información, depende por tanto de los sistemas TI (Tecnologías de Información) para alcanzar sus objetivos estratégicos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad, o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a las incidencias.

Los sistemas TI deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Sistema de Gestión de la Seguridad de la Información Corporativo (SGSI) donde se encuentran integrados los requisitos del Esquema Nacional de Seguridad (ENS), **SEIDOR** realiza un seguimiento continuo de los criterios y requisitos establecidos en la legislación que le es de aplicación, como el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), el Reglamento de la Unión Europea 2016/679 relativo a la protección del tratamiento de datos personales (RGPD) y normas internacionalmente reconocidas como son la ISO 27001 y la ISO 20000-1, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a las incidencias para garantizar la continuidad de los servicios prestados.

Según, lo que establece el propio RD 3/2010 en su artículo 10 la existencia de tres figuras diferenciadas que forman parte, siendo:

- **Responsable de la información** → Determinará los requisitos de la información tratada.
- **Responsable del servicio**→ Determinará los requisitos de los servicios prestados.
- **Responsable de seguridad**→ Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

SEIDOR debe asegurar que la seguridad de la información es una parte integral de cada etapa del ciclo de vida de los sistemas TI, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de

seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en propuestas de externalización de proyectos de TI.

2 OBJETO

SEIDOR define la presente Política de Seguridad de la Información como objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a las incidencias que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve a **SEIDOR** para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- **Disponibilidad:** propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- **Integridad:** propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- **Confidencialidad:** propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- **Autenticidad:** propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- **Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en **SEIDOR** serán:

- Velar por la seguridad de la información, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de disponibilidad y continuidad de la actividad que se definan para los distintos servicios ofrecidos por la organización.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

La Política de Seguridad:

- Se aprobará formalmente por la Dirección General.
- Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Se comunicará a todos los empleados y empresas externas qué trabajen con SEIDOR.

3 MISIÓN

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de **SEIDOR.**

- SEIDOR reconoce expresamente la importancia de la información, así como la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad de la organización, o al menos suponer daños muy importantes, si se produjera una pérdida total e irreversible de determinados datos.
- SEIDOR implementa, mantiene y realiza un seguimiento de los controles contenidos en su declaración de aplicabilidad y los procesos del SGSI, conforme a las normas ENS, RGPD, LOPDGDD, ISO 27010 e ISO 20000-1 principalmente, y cumple con todos los requisitos legales aplicables.
- La información y los servicios están protegidos contra pérdidas de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Los controles serán proporcionales a la criticidad de los activos a proteger y a su clasificación.
- La responsabilidad de la seguridad de la información involucrada en la prestación de los servicios incluidos en el alcance es de la Dirección General, que pondrá los medios adecuados, sin perjuicio de que los empleados o usuarios asuman su parte de responsabilidad respecto a los medios que utiliza, según lo indicado en las políticas, normativas y en los procedimientos complementarios. En el punto 6 “Organización de la Seguridad” de este mismo documento se describen las funciones y responsabilidades del Comité de Ciberseguridad, que gestionará la seguridad de la información, y de sus miembros.
- Quienes desempeñen la función de Seguridad de la Información y otras de administración relacionadas, serán quienes administren la seguridad.
- Se ha identificado a los responsables de la información, que deberán promover el establecimiento de los controles y medidas destinadas a proteger los datos que la integran, especialmente los de carácter personal o críticos.

- Se ha establecido dentro de la normativa un sistema de clasificación de la información, con diferentes niveles.
- Se han establecido y puesto a disposición, los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y, en general, de cualquier activo de SEIDOR.
- Los aspectos específicos más relacionados con la información sobre datos personales están regulados por el conjunto de normas recogidas en este documento de seguridad y en la normativa interna o de otra índole a la que pueda remitir o que se cite.
- Quienes no cumplan lo determinado en estas normas y en los procedimientos complementarios podrán ser sancionados de acuerdo con la legislación laboral y el convenio colectivo de referencia, o bien con sanciones personalizadas si están vinculados a SEIDOR bajo contratos no laborales, de acuerdo con las cláusulas que figuren en dichos contratos y la legislación aplicable en este último caso.
- Se realizan periódicamente evaluaciones de riesgos y, en función de las debilidades, se determina si es necesario elaborar planes de implantación o reforzamiento de controles.
- Se fomenta la difusión de información y formación en seguridad a empleados y colaboradores, previniendo la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar su posible existencia lo antes posible, y en caso de que existieren, procurándose una difusión muy restringida de las indagaciones.
- El personal de SEIDOR deberá conocer las normas, reglas, estándares y procedimientos relacionados con su puesto de trabajo, así como sus funciones y obligaciones, además de la separación de funciones y la revisión independiente de los registros, cuando sea necesario, de quién ha hecho qué, cuándo y desde dónde.
- Las incidencias de seguridad se comunican y tratan apropiadamente.

4 ALCANCE

La presente Política de Seguridad se aplica a todas las empresas que componen el grupo de empresas de **SEIDOR** y a sus sistemas y activos de información:

- A todos los departamentos, tanto a sus directivos como a empleados.
- A los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la organización.
- A bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- A la información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.

- A la información cedida dentro de un marco legal establecido, que será considerada como propia a efectos exclusivos de su protección.
- A todos los sistemas utilizados para administrar y gestionar la información, sean propios o alquilados o licenciados por la misma.

5 MARCO NORMATIVO

El control de la normativa y legislación de aplicación de esta política de seguridad que se incluye dentro del Sistema de Gestión de la Seguridad de la Información de SEIDOR, se gestiona en el registro "RE27.02_NORMATIVA_SEGURIDAD_INFORMACION", en el que se referencian entre otras las siguientes normativas y leyes:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).
- Ley Orgánica de Protección de Datos y garantías de los derechos digitales Ley 03/2018 (LOPDGDD).
- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica. BOE de 29 de enero de 2010.
- El CODIGO PENAL. LEY ORGÁNICA 10/1995, DE 23 DE NOVIEMBRE, del Código Penal.
- La Ley de Enjuiciamiento Criminal es de atención por contener en el Libro II, Título VIII, Capítulo. Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

Dicho marco normativo puede conllevar actualizaciones, por cambios legislativos. Por tanto, en normativa interna se creará un anexo de la política para establecer todas las actualizaciones del Marco normativo. Dichas actualizaciones se efectuarán con rango de Normativa Corporativa.

6 CONTENIDO

6.1 Gobierno Normativo

Seidor establece un cuerpo normativo alrededor de la Seguridad de la Información para permitir desplegar todos aquellos recursos normativos que permitan las capacidades y protección jurídica para dar respuesta a la misión que establece la Dirección General.

Para obtener esta eficiencia se establece un sistema que se gestionar en tres niveles principales funcionales: el estratégico, el táctico y el operacional. Además, se añade un nivel técnico para adaptar la norma a las evoluciones tecnológicas de los Sistemas de la Información.

Los siguientes son los tres niveles presentes en un sistema de planificación, más el nivel técnico adaptado a los recursos de los Sistemas de la Información:

6.1.1 Nivel estratégico o Nivel superior

Corresponde a la planeación que se orienta a lograr los objetivos de la organización y su fin es establecer los planes de acción para el funcionamiento de la compañía. Se basa en decidir los objetivos de la empresa, definir los recursos que se usarán y las políticas para obtener y administrar dichos recursos.

Este nivel establece el marco de referencia general, pero no detallado, para el funcionamiento de SEIDOR.

El nivel estratégico es conducido por el Comité Corporativo de Ciberseguridad, a través de su Dirección General Adjunta que lo representa y aprueba.

La validación, como aprobación final documental, recae en la Dirección General.

6.1.2 Nivel táctico o Nivel medio

Desarrolla detalladamente la planeación del funcionamiento de cada una de las áreas de SEIDOR a partir del marco de referencia elaborado en el nivel estratégico.

Este nivel es redactado por el director responsable de un área, aprobado por el comité y validado por la Dirección General Adjunta del Comité Corporativo de Ciberseguridad.

La diferencia básica con el nivel estratégico es que el primero se refiere a una política que afecta a toda la empresa y se extiende en el tiempo, mientras que la segunda se refiere a una norma específica en el uso de un producto, servicio, funcionamientos generales, métrica de calidad u otras que ofrece la organización con tiempos y plazos determinados.

6.1.3 Nivel Operativo o Nivel inferior

Corresponde a normas internas que permiten poder ejecutar tareas de forma coordinada con otros departamentos de SEIDOR que componen la compañía. Se desarrolla a partir de los lineamientos proporcionados por los niveles de planeación estratégico y táctico.

Este nivel es creado y aprobado por directores responsables de las áreas y, para su conocimiento, es elevado al Comité Corporativo de Ciberseguridad.

Los encargados de redactar esta documentación deben seguir las normas superiores y acatar reglas definidas con precisión por parte de los otros dos niveles.

La norma interna de este nivel cubre periodos de tiempo específicos de acuerdo con cada proceso.

6.1.4 Nivel funcional o Nivel Técnico

Corresponde a documentación técnica que permite a un trabajador poder utilizar una herramienta de los Sistemas de Información de Seidor que se esté implementando para dar servicio al trabajador

La creación depende de un responsable y su publicación solo deberá constar en la INTRANET de SEIDOR

6.2 Estructura normativa

Para ello se establece el siguiente cuerpo normativo, de mayor rango a menor:

- Nivel Superior o Estratégico
  - Política Corporativa
- Nivel Medio o Táctico
  - Normativa Corporativa
- Nivel Inferior u Operativo:
  - Procedimientos Corporativos
- Nivel Técnico:
  - Guías Técnicas
  - Manuales internos
  - Manuales de fabricantes

6.3 Políticas

SEIDOR debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidencias, de acuerdo con las políticas establecidas en el SGSI y los acuerdos de niveles de servicios comprometidos con sus clientes y usuarios.

Además, en el presente documento, trataremos como SEIDOR encara las políticas de la Seguridad de la Información, como organiza la seguridad en la corporación, como garantiza y protege los datos de carácter personal, la gestión del riesgo y el desarrollo de la política de la seguridad de la información.

6.4 Prevención

SEIDOR se compromete a poner todos los medios a su alcance para evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidencias de seguridad. Para ello se implementarán las medidas necesarias de seguridad determinadas por la legislación que le es de aplicación, los controles estimados como necesarios establecidos en el ENS, la ISO 27001 y la ISO 20000-1, así como cualquier control adicional identificado a través de su evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados en el SGSI.

Para garantizar el cumplimiento de la presente política, **SEIDOR** pondrá los medios organizativos y técnicos necesarios para:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Garantizar que los riesgos a los que puede verse afectados **SEIDOR** están identificados y se encuentran bajo niveles aceptables.
- Asegurar que los servicios que presta **SEIDOR** a sus clientes y las actividades que desarrolla para su prestación, poseen un creciente nivel de seguridad y han pasado por las pruebas necesarias para garantizar un nivel de riesgo aceptable.
- Desarrollar e implantar todas aquellas políticas, controles y normas necesarias en materia de seguridad de la información para garantizar el cumplimiento de los requisitos del negocio, los acuerdos de niveles de servicio comprometidos y las expectativas de las personas interesadas.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

6.5 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidencias, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua, para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya prestablecido como normales.

6.6 Respuesta

SEIDOR:

- Establece mecanismos para responder eficazmente a las incidencias de seguridad gestionados por la Oficina de Ciberseguridad Corporativa de Seidor (OCC).
- Pone a disposición de sus clientes y usuarios un punto de contacto para las comunicaciones de incidencias detectadas en sus operaciones, el Centro de Atención y Servicios de SEIDOR (cass.seidor@seidor.es).
- Establece en los modelos de relación protocolos de intercambio de información relacionada con incidencias con clientes y proveedores.

6.7 Recuperación

Para garantizar la disponibilidad de los servicios críticos, **SEIDOR** ha desarrollado planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

7 ORGANIZACIÓN DE LA SEGURIDAD

SEIDOR establece una definición de los siguientes Comités y Roles generales relacionados con su participación en la gestión y supervisión de **la seguridad de la información.**

- Comité de Dirección de Ciberseguridad - CDC
- Comité Corporativo de Ciberseguridad - CCC
- Comité de Crisis - CC
- Oficina de Proyectos Corporativos – OPC
- Oficina de Ciberseguridad Corporativa – OCC
- Comité de Protección de Datos – CPD
- Oficina de Protección de Datos – OPD
- Director de la Seguridad de la Información- Chief Information Security Officer- CISO
- Director de los Sistemas IT- Chief Information Officer - CIO
- Delegado de Protección de datos - DPO

7.1 Comité de Dirección de Ciberseguridad

El Comité de Dirección de ciberseguridad (CDC) de Seidor, está compuesto por los máximos representantes de la Dirección General de **SEIDOR**, los miembros del Comité Corporativo de Ciberseguridad (CCC), junto con el grupo de personas identificadas que por su rol o ámbito competencial gobiernan las distintas áreas/unidades de negocio y de gestión de **SEIDOR** a

propuesta del Comité Corporativo de Ciberseguridad (CCC) y ratificados por la Dirección General.

Con las siguientes competencias y atribuciones:

- Aprobar la Política de la Seguridad de la Información
- Nombramiento de los responsables: CIO, CISO, DPO, etc.
- Transmitir al Comité Corporativo de Ciberseguridad, los requerimientos, objetivos y necesidades funcionales en materia de ciberseguridad en base a su organización y necesidades operativas.
- Difundir y comunicar a las personas integrantes de sus ámbitos de operación, de las políticas, normas y buenas prácticas establecidas en materia de ciberseguridad.
- Colaborar con el Comité Corporativo de Ciberseguridad en el diseño, implantación, revisión y mejora de las políticas y procesos en materia de ciberseguridad y el SGSI, dentro de su ámbito de competencia.
- Colaborar con la Oficina de Ciberseguridad Corporativa de Seidor (OCC) en todos los procesos de investigación en materia de ciberseguridad dentro de su ámbito de competencia.
- Colaborar con la OCC en el proceso de gestión de riesgos y mantenimiento del plan de riesgos dentro de su ámbito de competencia.

7.2 Comité Corporativo de Ciberseguridad de SEIDOR

El Comité Corporativo de Ciberseguridad (CCC) de **SEIDOR**, se ha constituido por iniciativa directa de su Dirección General y se constituye como órgano colegiado para liderar y coordinar la seguridad de la información en **SEIDOR**, velar por el gobierno y la gestión de los riesgos de ciberseguridad, y emprenda acciones para la salvaguarda y mitigación de estos.

7.2.1 Misión

La misión del Comité Corporativo de Ciberseguridad(CCC) de Seidor es apoyar los objetivos y metas de todas y cada una de las empresas que componen el grupo **SEIDOR**, proporcionando liderazgo para garantizar la legalidad, confidencialidad, integridad, disponibilidad y trazabilidad de sus recursos de información, así como velar por el no compromiso de activos de terceros (Clientes) accesibles por la actividad propia que desarrolla **SEIDOR** con sus sistemas de información (de manera presencial o remota).

Entendemos por información:

- La propia información, como datos gestionados en los sistemas que la soportan, transmitidos a través de procesos digitales (redes, aplicaciones o cualquier tipo de mecanismo utilizado para la interoperabilidad con los sistemas objeto) o que se almacenen en dispositivos de almacenamiento, ya sean propiedad de Seidor o de terceros.
- Los procesos, aplicaciones y sistemas de información que los soportan y que son objeto de actividad propia que desarrolla Seidor.

En definitiva, la concienciación de todo el personal de **SEIDOR** acerca de los riesgos en materia de ciberseguridad, la protección de los recursos de información de **SEIDOR**, la investigación del posible mal uso de los sistemas, la supervisión del cumplimiento de todas las políticas establecidas, los procedimientos y las normas relativas al uso aceptable y adecuado de los recursos, así como el gobierno de los mecanismos de seguridad que se deriven para la protección y defensa de los sistemas objeto ante las amenazas tecnológicas que pudieran materializarse y comprometer el negocio propio o de terceros.

El Comité Corporativo de Ciberseguridad pertenece a los órganos de gestión y servicios transversales que **SEIDOR** presta a todas las empresas y divisiones pertenecientes al grupo, en dependencia directa de la Dirección General que es la responsable de la formalización de las políticas y de los objetivos en materia de ciberseguridad de **SEIDOR**, alineados con los objetivos estratégicos de la compañía.

7.2.2 Objetivos y funciones

El **Comité Corporativo de Ciberseguridad** tendrá los siguientes objetivos y funciones:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de SEIDOR en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de los diferentes departamentos 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.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección General.
- Aprobar la normativa de seguridad de la información.
- Aprobar los requisitos de formación y cualificación de los responsables de áreas, técnicos y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por SEIDOR y recomendar posibles actuaciones respecto de ellos.
- Velar por la coordinación de los diferentes departamentos en la gestión de incidencias de seguridad de la información.

- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de SEIDOR. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes departamentos.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Informar regularmente del estado de la seguridad de la información a la Dirección, mediante informes mensuales (Informes Corporativos de CIBERSEGURIDAD) y actas de reunión

7.2.3 Gobierno y organización del Comité Corporativo de Ciberseguridad

El Comité Corporativo de Ciberseguridad se constituye como un órgano colegiado, en dependencia directa de la Dirección General de **SEIDOR**, conforme a la siguiente **estructura organizativa:**

- **Estructura, PERMANENTE y OBLIGATORIA,** formada por los siguientes integrantes:
  - Dirección General o por delegación, mediante la figura del Director General Adjunto
  - Director de la Seguridad de la Información (CISO/CSO)
  - Director de los Sistemas TI (CIO)
  - Responsable del Centro de Procesamiento de Datos (CPD)
  - Representante de la OCC en funciones de secretario de acta
- **Según la materia a tratar**, se añaden los siguientes integrantes:
  - Responsable del SGSI
  - Responsable del Servicio afectado/comprometido
  - DPO
  - Director de Operaciones de Negocio
  - Otros perfiles de responsabilidad para tratar asuntos específicos

Representante de la dirección general: Persona perteneciente a la Dirección General de SEIDOR que, entre otras competencias de su cargo, velará por las siguientes actividades propias del Comité Corporativo de Ciberseguridad y el SGSI de Seidor:

- El establecimiento de la política y los objetivos de ciberseguridad y que estos sean compatibles con las políticas y objetivos estratégicos de SEIDOR.

- Adecuación en forma y grado de las decisiones acordadas por la Dirección General en relación asuntos relacionados con la Seguridad de la Información.
- La integración de los requisitos del sistema de gestión de ciberseguridad en los procesos de SEIDOR.
- La disponibilidad de los recursos necesarios para el SGSI y la actividad del Comité Corporativo de Ciberseguridad.
- La comunicación eficaz de las políticas y buenas prácticas en ciberseguridad dentro de la organización de SEIDOR.

Director de la Seguridad de la Información: CISO/CSO, en dependencia directa de la Dirección General de **SEIDOR**, que entre otras tendrá las siguientes competencias:

- Liderar la reunión donde se trate la ciberseguridad en SEIDOR, integrando a las personas de los distintos equipos involucrados, y adaptando la respuesta a las directrices estratégicas que se establezcan desde la Dirección General y al cumplimiento de la legislación vigente relacionada.
- Trasladar los proyectos que liderar en el diseño, implantación, revisión y mejora de los procesos de la Oficina de Ciberseguridad de SEIDOR (OCC).
- Evaluar en comité la calidad de las acciones y procesos de la OCC, ocupándose de la identificación de oportunidades de mejora, que reporta a través de los informes de gestión de la OCC.
- Convocar, preparar la agenda y documentar el acta de las reuniones del Comité.
- Asesorar sobre los aspectos de ciberseguridad a la Dirección General.
- Proporcionar asistencia a la Dirección General, identificando objetivos específicos de ciberseguridad.
- Dar traslado de los planes que se están elaborando, documentando y manteniendo sobre el plan de gestión de riesgos de ciberseguridad junto con el responsable del SGSI.
- Garantizar que el comité tenga conocimiento del estado de los medios establecidos para la supervisión de la ciberseguridad y proponer a aprobación para pilotar la mejora mediante proyectos internos con coste indirecto de la organización.
- Asesorar al Comité Corporativo de Ciberseguridad en el ámbito tecnológico y de servicios de ciberseguridad y colaborar en la toma de decisiones de esta.

Director de Sistemas TI de SEIDOR: Es la persona que dentro de la organización de **SEIDOR** gobierna los servicios TI internos y las infraestructuras que los soportan, que entre otras tendrá las siguientes competencias:

- Asesorar al Comité Corporativo de Ciberseguridad en el ámbito tecnológico de sistemas de información y de servicios de TI y colaborar en la toma de decisiones de este.

- Asesorar al Comité Corporativo de Ciberseguridad en materia de capacidad, disponibilidad y continuidad de los servicios internos de TI de SEIDOR y los sistemas que los soportan.
- Asesorar e informar al Comité Corporativo de Ciberseguridad de los cambios y proyectos en marcha en las infraestructuras y sistemas de TI que soportan los servicios de TI de SEIDOR.
- Facilitar la implementación de las medidas de seguridad físicas y lógicas que se establezcan en los planes de seguridad de SEIDOR.
- Facilitar y apoyar las tareas de análisis de riesgos de ciberseguridad.
- Implementar y mantener los sistemas de monitorización de los sistemas de información de SEIDOR.

7.3 Comité de Crisis

El Comité de Crisis (CC) es una figura potestativa que representa la Dirección General, táctica y de decisión clave en la gestión de cualquier situación de crisis que proceda de un **incidente de Seguridad MUY GRAVE.**

El CC es el encargado de decidir qué se hace y cómo se hace para la resolución del problema y qué se dice y cómo se dice en todo lo concerniente a su gestión comunicativa.

En el Comité de Crisis es el responsable de la actuación ante los acontecimientos que surjan durante la gestión de la crisis.

El Comité de Crisis debe tener desarrollado un manual de crisis para poder abordar con más éxito los incidentes de Seguridad.

7.3.1 Objetivos y funciones

A) Objetivos:
- Órgano decisorio para la gestión unificada de una situación de crisis
- Su principal cometido es acelerar el proceso de toma de decisiones para solventar incidencias y/o crisis definiendo las prioridades, estableciendo la estrategia y la táctica a seguir.
- Deberá, ante lo ocurrido, definir los principales escenarios a tener en cuenta y cómo actuar.

B) Funciones:
- Decidir o no si se trata de una situación de crisis y de qué tipo de nivel o grado es en función del sistema de alertas y de los niveles de gravedad previamente definidos.
- Decidir si se actúa o no ante ese problema. En caso afirmativo, decidir qué se hace.
- Establecimiento de las medidas para solucionar el problema y su ejecución.
- Repartir responsabilidades dentro de las áreas de gestión del problema para facilitar su resolución y la coordinación entre todas las partes que la integran.

- Proteger la imagen pública y reputación del impacto negativo que pueda tener la situación.
- Establecer toda la política informativa durante la situación de crisis.
- Ir evaluando en cada momento la estrategia que se lleva a cabo, sus acciones y resultados.
- Detectar y prever acontecimientos y pasos a seguir en función del desarrollo de los hechos.
- Centralizar la información tanto en el plano interno como externo.
- Dotar de coherencia y unidad a todas las acciones llevadas a cabo en los diferentes niveles de intervención que sean necesarios.
- Asignación de los portavoces internos y externos.

7.3.2 Gobierno y organización

El Comité lo convocara la Dirección General a petición propia o de un responsable

Un Comité de Crisis debe estar integrado por responsables de diferentes áreas de SEIDOR, y en concreto:

- Director General
- Director General Adjunto: Comunicación exterior
- Director General Adjunto: Relaciones Clientes/Proveedores
- Director General Adjunto: Relaciones Internacionales u otras empresas del grupo
- Director de RRHH
- Dirección de Marketing
- Dirección Financiera
- Dirección de Seguridad Corporativa
- Dirección de Sistemas IT
- Dirección Legal
- DPO

Dependiendo de la crisis, bajo decisión de la DG, se podrá crear el comité con las personas concretas que se requieran sin hacer participar todos sus integrantes.

En la primera reunión, dependiendo la materia, se debe designar por la Dirección General:

- Portavoz coordinador del Comité de Crisis que será la persona encargada de convocar, coordinar y dirigir el CC.
- Portavoz externo, la cara visible, de SEIDOR (puede, según cada caso coincidir que sea el portavoz coordinador), así como portavoz suplemente y también el portavoz interno de comunicación.
- Participación de personas ajenas a la empresa como asesores jurídicos (aunque ya exista un equipo jurídico interno), técnicos y especialistas según el problema y consultores de comunicación.

7.4 Oficina de Proyectos Corporativos – OPC

Este tipo de oficina tiene como función principal en recopilar información de los proyectos, monitorizar su ejecución para asegurar el correcto alineamiento de los proyectos con la estrategia de ciberseguridad de SEIDOR, asegurando la obtención de resultados óptimos en la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la Información

Dicha oficina, desarrollada en normativa interna, ha de asegurar que los proyectos se realizan de la misma forma con independencia del departamento que esté involucrado.

Las responsabilidades de una oficina de dirección de proyectos pueden abarcar desde el suministro de funciones de soporte para la dirección de proyectos hasta la responsabilidad de la dirección directa de un proyecto. Entre sus funciones, la oficina puede proporcionar:

- Servicios de apoyo administrativo, tales como políticas, metodologías y plantillas.
- Capacitación, mentoría y asesoría a los directores del proyecto.
- Apoyo al proyecto, alineamientos y capacitación sobre la dirección de proyectos y el uso de herramientas.
- Alineación de los recursos de personal del proyecto.
- Centralización de la comunicación entre directores del proyecto, patrocinadores, directores y otros interesados.
- Actualizar la aplicación de gestión de proyectos

7.5 Oficina de Ciberseguridad Corporativa

La Oficina de Ciberseguridad Corporativa de **SEIDOR** (OCC) es una unidad operativa, en dependencia directa del Comité de Ciberseguridad y cuya dirección la ejerce el CSO/CISO de **SEIDOR**, es responsable de la ejecución y seguimiento de todas las acciones y políticas en materia de ciberseguridad de las empresas del grupo **SEIDOR**.

7.5.1 Objetivos y funciones

La **Oficina de Ciberseguridad** Corporativa tendrá los siguientes objetivos y funciones:

- Elaborar los requisitos de formación y cualificación de los responsables de áreas, técnicos y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por SEIDOR y recomendar posibles actuaciones respecto de ellos.
- Analizar riesgos de ciberseguridad y proponer salvaguardas.
- Monitorizar el desempeño de los procesos de gestión de incidencias de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de los diferentes departamentos en la gestión de incidencias de seguridad de la información.

- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales de Seguridad que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Conjuntamente con el equipo del SGSI, la realización y revisión periódica del análisis de riesgos de los sistemas de TI.
- Seguimiento de los proyectos de las medidas de mitigación y salvaguardas de los riesgos evaluados.
- Respuesta a los Incidentes de Ciberseguridad: Investigación y análisis de los incidentes de ciberseguridad corporativa mediante el Equipo de Respuestas a Incidentes (ERI)
- Asesorar al Comité Corporativo de Ciberseguridad en el ámbito tecnológico y de servicios de ciberseguridad.
- Comunicación con las partes interesadas internas y externas en materia de ciberseguridad (occ@seidor.es)
- Comunicaciones globales a toda la empresa, que tenga relación directa o indirecta, relacionadas con la Ciberseguridad y la Seguridad de la Información que implique a la compañía i/o sus trabajadores

7.5.2 Gobierno y organización de la Oficina de Ciberseguridad Corporativa (OCC)

La Dirección de Seguridad Corporativa, mediante figura del Director de Seguridad de la Información (CISO), ostenta el gobierno y responsabilidad de la Oficina de Ciberseguridad Corporativa (OCC) para todo el grupo de empresas de SEIDOR.

La OCC está compuesta por los siguientes roles y equipos operativos:

- Equipos:
  - Equipo de Respuestas a Incidentes (ERI)
  - Nivel 3 Corporativo dentro del Cibersecurity Operations Center (CSOC)
  - Analistas Técnicos especializados en Ciberseguridad Corporativa: Ciberinteligencia, Seguridad Redes, Infraestructura y Aplicaciones.
- Roles:
  - Responsable/s Senior/s en Ciberseguridad
  - Analista/s en Ciberseguridad
  - Responsable/s en Respuesta a Incidentes de Seguridad
  - Analista/s en Ciberinteligencia
  - Analista/s en arquitectura de Seguridad de Redes
  - Analista/s en seguridad de sistemas
  - Analista/s en seguridad de aplicaciones
  - Analista/s en seguridad de Infraestructuras

7.6 Comité de protección de datos

SEIDOR para garantizar la correcta gestión de los tratamientos de datos personales, ha conformado en dependencia de la Dirección General el "Comité de protección de datos personales", que asumirá las responsabilidades del Sistema de Gestión de Protección de Datos Personales.

7.6.1 Objetivos y funciones

El Comité de protección de datos personales tendrá los siguientes objetivos y funciones

- Diseñar, implantar y supervisar los procesos del Sistema de Gestión de Protección de Datos Personales de SEIDOR
- Supervisar el registro de tratamientos de datos personales de la compañía.
- Informar y asesorar de las obligaciones en materia de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en la LOPDGDD y el RGPD.
- Asesorar en la evaluación de impacto relativa a la protección de datos personales.
- Supervisar el cumplimiento e implantación de las medidas de mitigación de riesgos identificadas.
- Supervisar la investigación de incidencias de protección de datos personales.
- Cooperar y actuar como punto de contacto con la Agencia Española de Protección de Datos (AEPD).

7.6.2 Gobierno y organización del Comité de Protección de Datos

El Comité de protección de datos personales está compuesto por los siguientes roles y equipos operativos, donde se ha buscado la representación de aquellas áreas que tienen un mayor impacto en su gestión y tratamiento:

- Representante de la Dirección General
- Representante del área jurídica
- Representante del área de recursos humanos y gestión de personal
- Representante del área de calidad
- Representante de Ciberseguridad Corporativa
- Representante del área de marketing y comunicación
- Responsable de administración de los sistemas corporativos
- Delegado de protección de datos personales (DPD)
- Oficina de Protección de Datos

7.7 Oficina de Protección de Datos (OPD)

La Oficina de protección de datos es una unidad operativa, dependiente del Comité de protección de datos personales, con los siguientes objetivos y funciones:

- Gestionar las comunicaciones en materia de protección de datos personales con las partes interesadas internas y externas (opd@seidor.es).
- Diseño, elaboración y actualización de los procedimientos del sistema de gestión de protección de datos.
- Asesorar al personal de SEIDOR en materia de protección de datos personales, así como la revisión de los contratos de encargado de tratamiento.
- Gestionar el registro de tratamientos de datos personales
- Realizar y mantener el análisis de riesgos en protección de datos y los estudios de impacto de aquellos tratamientos que lo requieran.
- Gestionar las solicitudes de derechos de los titulares de los datos personales
- Elaborar contenidos formativos en esta materia.
- Coordinar las acciones de formación.
- Coordinar las acciones de mitigación de los riesgos evaluados
- Informar al Comité de protección de datos de las acciones acometidas, el estado de los proyectos en marcha, proponer acciones de mejora y de mitigación de riesgos.

7.8 Roles: Funciones y Responsabilidades

En el caso de **SEIDOR** todas las responsabilidades recaen en la Dirección General, donde se encuentran la propiedad de la sociedad y las personas pertenecientes a la Dirección General Adjunta.

SEIDOR deberá garantizar, como mínimo, de la existencia de tres figuras diferenciadas para cada sistema en base las responsabilidades siguientes:

- Responsable de la información
- Responsable del servicio
- Responsable de seguridad

Siendo la figura de responsable de Seguridad, designada y supervisada por el CISO de la compañía.

El Responsable de la Información y Responsable del Servicio dependerá de la Dirección General.

Las funciones y responsabilidades se detallan a continuación:

A) Responsable de la Información

- Velar por el buen uso de la información de su competencia y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad, de la información de la que es responsable.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

B) Responsables del Servicio

- Establecer los requisitos de los servicios en materia de seguridad que deban ser garantizados en el tratamiento de la información, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Valorar para cada servicio contemplado en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).
- Establecer los requisitos del servicio, de su competencia, en materia de seguridad
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.
- Trabajar en colaboración con el Director de Seguridad de la Información en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

C) Responsable de Seguridad: El Director de Seguridad de la Información

El director de seguridad de la información es el CISO (Chief Information Security Officer)

Se encargará de la designación y supervisión de los responsables de seguridad de los diferentes sistemas.

En anexo a esta política se establecerá en documento, un control de las personas que están designadas con los roles y equivalencias correspondientes.

El rol desempeñado a nivel ejecutivo dependiendo del CEO y su función principal es:

- Alinear la estrategia de seguridad de la información con los objetivos de la organización
- Comunicar y coordinar las áreas operativas, actuando de enlace con la Alta Dirección en materia de seguridad de la información (estado de riesgos, planes de acción, amenazas, incidencias y control económico)
- Establecer métricas e indicadores de seguridad que permita a la organización conocer su nivel de seguridad actual, así como la mejora a futuro.
- Formar, concienciar y sensibilizar a la organización en materia de seguridad de la información

La figura de CISO dependerá del Director de Seguridad/CSO y las funciones concretas serán las siguientes:

- Definir las estrategias de la organización en seguridad de la información, asegurando que se alinean con el resto de las estrategias de la organización, y de que son aprobadas por la Dirección
- Desarrollar su ejecución bien directamente, o mediante la supervisión de otras áreas que están involucradas en dicha ejecución y mediante la coordinación con otras áreas de la organización.
- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Instar y asesorar en la valoración de los requisitos de seguridad que deban ser garantizados en el tratamiento de la información por parte de los nuevos servicios electrónicos prestados por SEIDOR
- Supervisar el estado de seguridad del sistema.
- Definir el mapa de riesgos de seguridad de SEIDOR: Realizar la evaluación de riesgos de Seguridad de la Información de la organización, incluyendo tanto las actividades de análisis de riesgo, como de evaluación de los mismos y preparación de los planes de tratamiento de riesgos derivados. En ocasiones, esta actividad cubrirá el total de gestión de riesgos de la organización.
- Realizar o promover las auditorías periódicas a las que obliga el SGSI, en el que se encuentra integrado el ENS, para verificar el cumplimiento de los requisitos de este.
- Identificar el nivel de riesgo aceptable para la Organización; es decir que umbral de riesgo está dispuesto asumir la Dirección General.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar un informe periódico de seguridad mensual, que incluya los incidentes más relevantes del periodo.
- Definir el marco de control normativo de seguridad (políticas, normas, guías, procedimientos)

- Promover la formación y concienciación en materia de seguridad de la información del personal de SEIDOR
- Comprobar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Aprobar los procedimientos o documentos que afecten a la seguridad de la información elaborados por el Responsable del Sistema
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Dirigir la Oficina de Ciberseguridad Corporativa OCC
- Recibir y analizar requisitos y objetivos de ciberseguridad.
- Analizar riesgos de ciberseguridad y proponer salvaguardas.
- Colaborar en la planificación de la ciberseguridad dentro de su dominio de competencia.
- Definir, implantar y liderar la respuesta ante incidentes de seguridad de la información en la organización
- Coordinar las medidas de contención y recuperación necesarias para resolver el incidente que se produzca y, si es preciso, invocar al equipo de Continuidad de Negocio implicado.
- Participar, ante incidentes de especial criticidad, que afecten de forma grave los compromisos y actividades de la organización, o que se prevea tengan importantes consecuencias derivadas, en el Comité de Crisis aportando su visión experta para lograr, de forma ágil, conocer la gravedad, implicaciones, su posible evolución, así como definir cuál debe ser el posicionamiento de la organización ante todos los stakeholders e impulsar una respuesta global desde una perspectiva estratégica,
- Implementar y mantener controles de ciberseguridad.
- Participar en estudios e investigaciones de ciberseguridad.
- Establecer los contactos pertinentes con reguladores, peers (sectoriales y multisectoriales), fuerzas y cuerpos del estado, fabricantes y proveedores estratégicos. Este punto es relevante pues contribuye a consolidar una red de inteligencia global permitiendo anticipar la identificación de amenazas en las organizaciones participantes
- Establecer los canales de reporte y colaboración con autoridades y reguladores, CISRTs de interés y fuerzas y cuerpos de seguridad del Estado.
- Denunciar ante las autoridades competentes un ciberataque.
- Realizar o coordinar análisis forenses, y en su caso, los informes periciales. Así como defenderlos en sede judicial (si procede).
- Establecer y llevar a cabo la notificación de incidentes conforme a las distintas leyes y normativas.

- Informar/reportar a la Dirección General y cuando proceda: a autoridades competentes o en sede judicial.
- Coordinarse con otras figuras relevantes relacionadas con su ámbito de actuación tales como Protección de Datos, Área Jurídica, Auditoría, Riesgos Corporativos, Comunicación, Recursos Humanos.
- Coordinarse con centros de respuesta a incidentes.
- Colaborar en grupos de interés en esta materia.

D) Director de Sistemas TI (CIO)

Reporta directamente al CEO, y se encarga básicamente de que las estrategias de la organización estén alineadas con la tecnología de la información para lograr los objetivos planificados.

Además, se encarga de mejorar los procesos de tecnologías de la información de la organización, gestionar el riesgo y la continuidad de negocio, controlar el coste en infraestructura de tecnologías de la información, alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, y establecer mejoras e innovaciones de soluciones y productos.

Este rol estará representado por el CIO (Chief Information Officer) del grupo SEIDOR el cual podrá establecer, en base la dimensión de su organización de gestión, en las figuras señaladas en una RACI de ITILV4.

Las figuras que designará el CIO serán las siguientes: Administrador del Sistemas, Responsable de Sistemas, Responsable de Sistemas TI Corporativos.

La asignación de la responsabilidad debe efectuarse por escrito, donde consten las funciones y las responsabilidades. Este nombramiento debe comunicarse en Comité Corporativo de Ciberseguridad para su conocimiento y control.

Tales figuras serán las siguientes:

- **Administrador de Sistemas**
    - La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de Información de su competencia.
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de Información.

- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- La aplicación de los Procedimientos Corporativos de Seguridad.
- Aprobar los cambios en la configuración vigente del sistema de Información.
- Velar el cumplimiento de las medidas y controles de seguridad que aplican en los Sistemas durante las etapas de desarrollo, instalación y prueba del mismo.
- 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los Responsables de la Ciberseguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidencias de seguridad, desde su detección hasta su resolución.
- Colaborar con el Director de Seguridad en la implementación de las medidas de seguridad físicas y lógicas que se establezcan en los planes de seguridad de SEIDOR.
- Establecer planes de contingencia y los procesos de análisis y gestión de riesgos en el Sistema.
- Elaborar, actualizar y/o revisar los procedimientos de recuperación de los sistemas, asegurar mediante pruebas periódicas su vigencia y eficacia.
- Elaborar la documentación de seguridad del Sistema.
- Tener un papel activo en facilitar y apoyar las tareas de análisis de riesgos de ciberseguridad.
- Colaborar en implementar y mantener los sistemas de monitorización de los sistemas de información de SEIDOR.

- **Responsable de Sistemas**
  - Gestionar el sistema de Información de su competencia durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.

- Definir la tipología y los procedimientos de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir las políticas de acceso de usuarios al sistema.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el sistema y aprobar las modificaciones importantes de dicha configuración.
- Facilitar y colaborar en el análisis y gestión de riesgos en el sistema.
- Elaborar y/o revisar la documentación de seguridad del sistema.
- Determinar la categoría del sistema según lo establecido en el SGSI y determinar las medidas de seguridad que deben aplicarse.
- Implantar y controlar las medidas específicas de seguridad del sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Elaborar, actualizar y/o revisar los procedimientos de recuperación de los sistemas, asegurar mediante pruebas periódicas su vigencia y eficacia.

- **Responsable de Sistemas TI Corporativos**
  - Gobernar y gestionar los servicios y sistemas TI corporativos y las infraestructuras que los soportan durante todo su ciclo de vida, incluyendo las especificaciones, instalación y verificación de su correcto funcionamiento.
  - Definir la tipología y los procedimientos de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
  - Definir los criterios de uso y los servicios disponibles en los sistemas y servicios TI corporativos.
  - Definir las políticas de acceso de usuarios a los sistemas y servicios TI corporativos.
  - Realizar la documentación de seguridad de los sistemas y servicios TI corporativos.
  - Aprobar los cambios que afecten a la seguridad del modo de operación de los sistemas y servicios TI corporativos.

- Aprobar la configuración autorizada de hardware y software a utilizar en los sistemas y servicios TI corporativos y aprobar las modificaciones importantes de dicha configuración.
- Facilitar y colaborar en el análisis y gestión de riesgos en los sistemas y servicios TI corporativos.
- Revisar y aprobar la documentación de seguridad de los sistemas y servicios TI corporativos.
- Determinar la categoría del sistema según lo establecido en el SGSI y determinar las medidas de seguridad que deben aplicarse.
- Controlar las medidas específicas de seguridad de los sistemas y servicios TI corporativos.
- Establecer planes de contingencia y emergencia.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Revisar y aprobar los procedimientos de recuperación de los sistemas, asegurar mediante pruebas periódicas su vigencia y eficacia

E) Responsable del SGSI de SEIDOR

Es la persona perteneciente al departamento de calidad, responsable de la gestión y mantenimiento del SGSI de **SEIDOR** certificado en ISO 27001 e ISO 20000-1, Esquema Nacional de Seguridad, y otras certificaciones. Sus funciones principales serán las siguientes:

- Asegurar que el SGSI es conforme con la legislación vigente, los requerimientos y expectativas de las partes interesadas, las especificaciones de las normas internacionales ISO 27001 e ISO 20000-1, Esquema Nacional de Seguridad u otras certificaciones y mejoras continuas.
- Supervisar el desarrollo de los procesos y proyectos del SGSI, ejecutando tareas operativas y coordinando a otros equipos y roles ejecutores en la operación de los procesos y proyectos.
- Apoyar y colaborar con el Director de Seguridad de la Información en todas sus funciones.

F) Delegado de Protección de Datos

Tiene las siguientes funciones y responsabilidades:

- Colaborar en establecer los requisitos de seguridad que deban ser garantizados en el tratamiento de la información de la que es responsable.

- Colaborar en la valoración para cada información contemplada en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).
- Trabajar en colaboración con el Responsable de Seguridad de la Información y el de los Sistemas de Información en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes y por su cumplimiento
- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y demás normativas en materia de protección de datos personales.
- Supervisar el cumplimiento de lo dispuesto en el RGPD y demás normativas en materia de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales.
- Colaborar en la Supervisión de la asignación de responsabilidades.
- Supervisar la concienciación y formación del personal que participa en las operaciones de tratamiento.
- Supervisar las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos.
- Supervisar su aplicación de conformidad con el artículo 35 del RGPD.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36.
- Realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

7.9 Procedimientos de designación

La Dirección General es (persona u órgano colegiado con responsabilidad unitaria identificable):

- Responsable de la Información
- Responsable del Servicio

También debe nombrar:

- El Director de Seguridad Corporativo (CSO), que formará parte y reportará al Comité Corporativo de Seguridad mediante la figura de Director de Seguridad de la Información (CISO).
- El Director de Sistemas TI (CIO) que formará parte y reportará al Comité de Seguridad.

El Director del departamento de Sistemas TI (CIO), podrá crear y designar roles específicos, para Corporación o Delivery, tales como:

- El Responsable del Sistema
- El Responsable de la Administración

El Director del departamento de Seguridad Corporativa (CSO), podrá crear y designar roles específicos tales como:

- El Director de Seguridad de la Información – CISO
- El Responsable de Seguridad de los sistemas
- El Responsable de la Oficina de Ciberseguridad Corporativa
- El Responsable del CSOC para dar servicios a la Corporación

Una vez designados, deben ser trasladados a la Dirección General mediante las estructuras funcionales de los comités.

7.10 Política de seguridad de la información

Será misión del Comité de Ciberseguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Dirección General y difundida para que la conozcan todas las partes afectadas.

8 DATOS DE CARÁCTER PERSONAL

La LOPDGDD y el RGPD, tratan de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, y resulta de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

La política de privacidad de **SEIDOR** que regula la normativa de protección de datos se encuentra publicada en http://www.seidor.es/content/seidorweb/es/politica.html.

Todos los sistemas de información de **SEIDOR** se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos para su tratamiento.

Para garantizar dicha protección, se han adoptado las medidas de seguridad que se correspondan con las exigencias previstas en la legislación de aplicación.

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con **SEIDOR.**

9 GESTIÓN DE RIESGOS

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

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité Corporativo de Ciberseguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité Corporativo de Ciberseguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis y Gestión de riesgos.

10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

10.1 Sistema de Gestión de Seguridad de la Información

El Sistema de Gestión de Seguridad de la Información (SGSI), dependen del CISO en cooperación con el Departamento de Calidad, que a su vez es responsable del Sistema Integrado de Gestión, del grupo de empresas de **SEIDOR.**

Para la correcta gestión del SGSI, **SEIDOR** gestiona y mantiene un sistema de control y aplicabilidad de una serie de controles según las normas de referencia ISO 27002 y el Esquema Nacional de Seguridad según las líneas estratégicas de **SEIDOR** y los alcances establecidos para las operaciones y las empresas del grupo, cada uno de estos controles se revisan periódicamente y se establecen sus niveles de madurez, así como los planes de implantación y mejoras necesarios, en base a la siguiente escala:

- **Nivel 0 Inexistente:** La organización no tiene una implantación efectiva del control ni de los procesos asociados:
    - Los procesos son generalmente ad-hoc y caóticos
    - El éxito depende de la competencia del personal y no del uso de procesos aprobados
- **Nivel 1 Inicial:** La organización implementa y alcanza los objetivos de los procesos. Este nivel de madurez busca que la organización implemente los resultados del control y/o el proceso:
    - Se implementan los controles/procesos requeridos para apoyar a los objetivos

de la organización.

- Se realizan un conjunto de actividades y tareas que alcanzan los objetivos y el propósito de dichos procesos.
- El propósito y objetivo de los procesos se corresponde con la parte específica de los procesos.

- **Nivel 2 Repetible pero intuitivo:** La organización gestiona los controles y procesos y los resultados de las actividades se establecen, controlan y mantienen:
  - Se establecen planes y procedimientos para realizar los procesos.
  - Se asignan responsabilidades y autoridades.
  - Se asignan los recursos y la información adecuada.
  - Se realiza un seguimiento respecto a planes y procedimientos.
  - Se Toma acciones para tratar las desviaciones.
  - Se identifican los requisitos para la gestión de los productos de trabajo de los procesos.
  - Se toman acciones para asegurar que los requisitos se cumplen.
  - Se asientan las bases metodológicas para poder medir la mejora real de los procesos.
- **Nivel 3 Proceso definido y en implantación:** La organización utiliza controles y procesos adaptados basado en estándares. Los procesos se describen según estándares, procedimientos, herramientas y métodos mediante guías de adaptación:
  - Se establecen descripciones de proceso estándar.
  - Se asegura que los procesos en los controles se adaptan a partir del conjunto de procesos estándar.
  - Se recogen y analizan los datos para comprender la eficacia del proceso adaptado.
  - Se utilizan los datos recogidos para mejorar el conjunto de procesos estándar y los procesos adaptados.
- **Nivel 4 Gestionado y medible:** La organización gestiona cuantitativamente los controles y procesos asociados:
  - Se establecen objetivos cuantitativos de rendimiento de los procesos alineados con los objetivos de seguridad de la información y del negocio.
  - Se seleccionan procesos para el análisis de rendimientos.
  - Se recogen almacenan y analizan datos sobre el rendimiento de los procesos seleccionados.
  - Se identifican causas especiales de variación en el rendimiento de los procesos y toma las acciones para eliminarlas.

- Se establece un rendimiento de los procesos estable, capaz y predecible dentro los límites de control definidos.

- **Nivel 5 Optimizado:** La organización mejora continuamente los procesos, basándose en una comprensión cuantitativa de las causas comunes de variación, para cumplir los objetivos de la seguridad de la información y del negocio:
  - Se identifican las causas comunes de variación del rendimiento de los procesos basándose en los resultados de los análisis e identifica mejoras.
  - Se identifican innovaciones para mejorar el rendimiento de los procesos y el éxito del control.
  - Se identifican oportunidades de mejora con el control de riesgos asociados
  - Se recoge y analiza datos para seleccionar mejoras para la organización, basadas en el impacto en el rendimiento de los procesos y en éxito del control.
  - Se utilizan las mejoras, controla el rendimiento de los procesos mejorados, y compara los resultados con los valores esperados.

10.2 Política de uso de los Sistemas de Información

La "Política interna de uso de los Sistemas de Información" se encuentra publicada en la intranet de **SEIDOR**, que tiene por objeto regular la utilización de los sistemas de información (SI) propiedad de **SEIDOR** puestos a disposición de sus trabajadores y usuarios, así como garantizar la seguridad, legalidad, rendimiento, integridad y privacidad de la información, preservar la privacidad y seguridad del personal y en general, garantizar el cumplimiento efectivo de las actividades y demás tareas que emanan del ámbito estrictamente labora. No se considera aceptable:

- La creación, uso o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de los equipos están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso intencionadamente. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.

- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus

10.3 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 requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información confidencial.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede.

Cuando se termine la relación laboral o contractual con empleados o personal externo, 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.

10.4 Seguridad física y del entorno

Para que una seguridad lógica sea efectiva, es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa.

10.4.1 Áreas seguras

SEIDOR tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.

La totalidad de las instalaciones de **SEIDOR** cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen y el acompañamiento del personal durante la estancia en las instalaciones.

10.4.2 Seguridad de los equipos

Los equipos informáticos son un activo importante del que depende la continuidad de las actividades, por lo que serán protegidos de manera adecuada y eficaz.

Los equipos informáticos de **SEIDOR** están protegidos contra posibles fallos de energía (ordenador portátil con batería, SAIs, etc.).

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad,

integridad y sobre todo 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. También será necesario adoptar las medidas de precaución necesarias en caso de los equipos deban abandonar las instalaciones para su mantenimiento.

10.5 Gestión de comunicaciones y operaciones

10.5.1 Procedimientos operativos y responsabilidades

SEIDOR controlará el acceso a los servicios en redes internas y externas y se asegurará que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red de **SEIDOR** y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red existirán mecanismos para limitar los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del dominio. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo con estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

En algunos casos será necesario que distintas áreas estén lógicamente separadas del resto para evitar accesos no autorizados.

10.5.2 Protección frente a código malicioso y código móvil

Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de **SEIDOR.**

Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado por la Oficina de Ciberseguridad y autorizado por el comité.

El Administrador del Sistema instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

10.5.3 Copias de seguridad

Los datos deben ser guardados según las normas establecidas en la Política de uso de los sistemas de información, para asegurar su disponibilidad.

10.5.4 Gestión de la seguridad de la red

Los elementos de red (switch, router...etc.) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema.

Existirá una gestión gráfica de la red de forma que su mantenimiento pueda resultar más cómodo.

10.6 Gestión de soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a los ficheros de donde han sido extraídos.

10.6.1 Intercambio de información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, fax, etc.).

10.6.2 Seguimiento

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos, así como para recomendar cualquier cambio que se estime necesario.

10.7 Control de accesos

10.7.1 Requisitos del servicio para el control de accesos

La información debe estar protegida contra accesos no autorizados. El Responsable del Servicio definirá las necesidades de acceso a la información a dos niveles, para el conjunto de áreas y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

10.7.2 Gestión de accesos de los usuarios

El administrador del sistema es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.

Cada usuario deberá estar asociado a un perfil, de acuerdo con las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a información y sistemas que no le son necesarios para las competencias de su trabajo.

10.7.3 Responsabilidades del usuario

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado, así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

10.7.4 Control de acceso a la red

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

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con **SEIDOR y** trasladarle las política, normas y procedimientos de seguridad que deban de adoptar, para mantener el mismo nivel de seguridad que si fueran empleados de la propia organización.

No se recomienda el uso de servicios de VPN gratuitos o terceros para acceder los sistemas de información de la compañía.

Se restringirá, siempre que sea posible, el acceso a los sistemas de información desde redes de anonimización (TOR, I2P, etc.) y otros servicios comúnmente utilizados para realizar acciones ilegales y cuya finalidad es la de ocultar el origen real de las conexiones.

10.7.5 Informática móvil y teletrabajo

Cuando los equipos o la información propiedad de **SEIDOR** están fuera de las instalaciones, es el empleado que los está utilizando el que debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

10.8 Gestión de incidencias

Las incidencias de Ciberseguridad que cualquier empleado observe o sospeche deben ser trasladadas a la Oficina de Ciberseguridad Corporativa mediante los medios que se faciliten para su comunicación, principalmente correo electrónico.

Para otra de seguridad, bien sea física (fuego, agua, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Centro de Atención y Servicios de **SEIDOR** (cass.seidor@seidor.es) 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.

10.9 Continuidad del servicio

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

Para garantizar la continuidad de la actividad en estos casos, **SEIDOR** establecerá planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

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

La gestión de la continuidad del servicio se incorporará a los procesos de **SEIDOR** y será responsabilidad de una o varias personas dentro de la entidad.

11 OBLIGACIONES DEL PERSONAL

Todos los miembros de **SEIDOR** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité Corporativo de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **SEIDOR** recibirán concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **SEIDOR,** en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12 TERCERAS PARTES

Cuando **SEIDOR** preste servicios a otras entidades u organismos o maneje información de estas, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités Corporativos de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidencias de seguridad.

Cuando **SEIDOR** utilice servicios de terceros o ceda información a terceros, se les hará partícipe 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.