POLÍTICA DE SEGURIDAD

AC CAMERFIRMA SA

CONTROL DE ACTUALIZACIONES

VERSIÓN	FECHA	ELABORADO	ACTUALIZACIÓN	BORRADOR	APROBADO
2.0	Mayo 2002	Mónica Díaz Prada		Ramiro Muñoz	Ramiro Muñoz
3.0	Septiembre 2002		Mónica Díaz Prada	Ramiro Muñoz	Ramiro Muñoz
4.0	Marzo 2004		Mónica Díaz Prada	Ramiro Muñoz	Ramiro Muñoz
5.0	Septiembre 2004		Rosario Márquez	Ramiro Muñoz	Ramiro Muñoz
6.0	Marzo 2005		Juanjo Pérez (InetSecur S.L)		
7.0	Junio 2006		Paloma Hernández (TB Security)	Ramiro Muñoz	Ramiro Muñoz
7.1	Abril 2007	Ramiro Muñoz			
7.1	Mar 2010	Ramiro Muñoz			
7.1.1	Feb2012	Ramiro Muñoz			
7.1.2	Mayo 2013		Ramiro Muñoz		
7.1.2	Dic-2016		Ramiro Muñoz		
7.2	Junio 2015	Auren		Ramiro Muñoz	Ramiro Muñoz
7.3	Mayo 2016	Auren		Ramiro Muñoz	Ramiro Muñoz
7.4	Julio 2017	AUREN	AUREN	AUREN	Ramiro Muñoz
7.4.1	Noviembre 2018		Ramiro Muñoz		

CONTROL DE CAMBIOS

DESCRIPCIÓN DEL CAMBIO	APARTADOS QUE CAMBIAN RESPECTO A VERSIÓN ANTERIOR
AÑADIDO	
MODIFICADO	Cambio del correo de aviso de incidencias de soporte a sistemas
ELIMINADO	

MANTENIMIENTO DEL DOCUMENTO

Se requiere mantenimiento y/o revisión de este documento cada vez que el Responsable de Seguridad (definido en el documento ***"07 - Funciones y responsabilidades del personal de Camerfirma"***) lo crea oportuno y, en todo caso, cuando se produzcan cambios en:

- la infraestructura tecnológica u organizativa de la Entidad
- la evaluación de riesgos preliminar (ver resultados en doc. **"Análisis de Riesgos-Resultados", código "CONF-2005-05-01 Resultados"**).

Cada vez que se emita una nueva versión de este documento, este debe ser:

- Aprobado por la Dirección General
- Comunicado a todos las partes interesadas (empleados, colaboradores, etc.) su disponibilidad en **gestor documental de la empresa (SFTP).**

VALIDEZ

Hasta su siguiente actualización.

TRATAMIENTO Y CONFIDENCIALIDAD

Documento de acceso interno

DISTRIBUCIÓN

Distribución al personal interno de Camerfirma y a las partes interesadas que lo requieran, a través del FTP seguro de la empresa.

Cada versión nueva se comunicará a los empleados mediante un correo electrónico desde el departamento de RRHH.

INDICE

1 INTRODUCCIÓN

Este es un documento interno que expresa el compromiso de la Dirección de la Entidad con la Seguridad de la Información.

Este documento conjuntamente con la **DPC (Practicas de certificación)** constituyen la base de la documentación de seguridad de AC Camerfirma. La **Declaración de Practicas de Certificación (DPC/ CPS en inglés)** de CAMERFIRMA define el conjunto de prácticas adoptadas por AC Camerfirma para la emisión de certificados digitales.

El presente Documento de Seguridad desarrolla normas y procedimientos sobre seguridad de la información, según los requerimientos marcados en la legislación española y en los estándares nacionales e internacionales sobre seguridad de la información de más amplio reconocimiento. Estos estándares se detallan más adelante, en la sección "C. AMBITO DE APLICACIÓN" de este documento.

Para la formulación de este conjunto de normas y procedimientos de seguridad informática, la Gerencia de CAMERFIRMA ha determinado previamente, además, cuáles son los objetivos de control que debe cubrir dicha normativa, en función de los riesgos que han sido identificados para su negocio (ver documento interno **"Análisis de Riesgos", código CONF-2005-05-01**.

Este documento constituye la base para el desarrollo de un conjunto de medidas específicas que se concretan en los Manuales de Procedimientos, a los que se hará referencia a lo largo de todo este documento.

2 DECLARACIÓN DE PRINCIPIOS

Es compromiso de la Dirección de Camerfirma proteger la información de la difusión, manipulación no autorizada o pérdida de la misma.

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción hasta su procesamiento, comunicación, transporte, almacenamiento y difusión a terceros.

Cada empleado tiene la obligación y el deber de proteger adecuadamente la información, conforme a las clasificaciones y estándares de la Sociedad, los cuales le serán comunicados a través de este documento y del documento de "ACEPTACIÓN DE RESPONSABILIDADES DEL PERSONAL INTERNO IMPLICADO EN EL "SISTEMA CAMERFIRMA".

3 OBJETIVO DE LA POLÍTICA DE SEGURIDAD

La Dirección de Camerfirma tiene la responsabilidad de proteger adecuadamente el activo que supone la información de amenazas tales como, errores, fraudes, malversaciones, sabotajes, terrorismo, extorsiones, espionaje industrial, violaciones de intimidad, interrupciones de servicio y desastres naturales.

Camerfirma intercambia información con terceros, denominados grupos de interés. Estos grupos incluyen a cualquier persona con interés en la manera en que Camerfirma protege su información. Por ejemplo, los propios empleados de Camerfirma tienen interés en que se mantenga la confidencialidad sobre su información personal.

Para proteger los intereses de estos grupos, Camerfirma ha desarrollado una política que contempla los objetivos de la Sociedad y las expectativas que la misma tiene sobre sus empleados y colaboradores externos. Las normas han sido desarrolladas para proporcionar una guía específica para los empleados y colaboradores y para asegurar la implantación de esta política de manera consistente en todas las áreas de la Sociedad.

Los siguientes **principios generales** son claves para lograr la protección de la información de Camerfirma:

- La información de Camerfirma y sus Sistemas de Información son activos críticos que deben ser protegidos para asegurar el funcionamiento de la Sociedad.
- La información de Camerfirma debe ser protegida conforme a su susceptibilidad, valor y criticidad.
- Todos los empleados y colaboradores de Camerfirma tienen la responsabilidad de proteger la información que se les ha confiado.
- La protección de la información permite el desarrollo del negocio de Camerfirma. Las medidas de protección deben desarrollarse conforme a una evaluación del riesgo.
- Toda información debe ser clasificada por el propietario en una de estas tres clasificaciones: **Confidencial, Uso Interno o Pública.**

Para determinar qué medidas de protección son necesarias, debemos asegurar la **confidencialidad, integridad y disponibilidad de la información** y clasificar la misma como Confidencial, Uso Interno o Pública, como se define en la sección Clasificación de la Información de este documento.

4 ALCANCE DE LA POLÍTICA DE SEGURIDAD

Esta política es **aplicable a todos los trabajadores de Camerfirma**, sean o no empleados, incluyendo cualquier persona ajena a Camerfirma que tenga acceso a la información gestionada o propiedad de la Sociedad. La política también es aplicable a toda la información en soporte digital y a los Sistemas de Información propiedad de la Sociedad o gestionados por la misma. La información de Camerfirma debe ser protegida conforme a su sensibilidad, valor y criticidad. Deben emplearse medidas de protección independientemente de:

- El soporte en que se almacena la información (cinta, disco, disquete, etc.).
- Los sistemas que la procesan (mainframes, PC's, teléfonos móviles, tabletas… etc.).
- Los métodos para comunicarla (correo electrónico, transmisión por la red, etc.).

5 PROGRAMA DE PROTECCIÓN DE LA INFORMACIÓN

El Programa de Protección de la Información es el **proceso** puesto en marcha por la Dirección de CAMERFIRMA para asegurar la protección de la información en sus tres vertientes más importantes: confidencialidad, integridad y disponibilidad.

A continuación se describen los aspectos más importantes de dicho programa.

5.1 RESPONSABLE DEL DESARROLLO DEL PROGRAMA DE PROTECCIÓN DE LA INFORMACIÓN

El **Responsable de Seguridad** es el encargado de promover el desarrollo y mantenimiento de dicho Programa, de asegurar su idoneidad y aplicabilidad conforme evolucionan la tecnología y las condiciones de la Sociedad.

5.2 CONCIENCIACIÓN Y EDUCACIÓN SOBRE EL ENTORNO DE SEGURIDAD DE LA INFORMACIÓN

Todo el personal de Camerfirma está implicado en la protección de la información y debe ser consciente de los recursos disponibles para asegurar esta protección. **El Responsable de Seguridad** se encargará de desarrollar un **programa de concienciación y educación** que proporcione la información necesaria a los empleados y colaboradores con acceso a la información de la Sociedad.

5.3 MEDIDAS DE ACTUACIÓN ESPECIALES

El Programa de Protección de la Información de CAMERFIRMA debe asegurar que la información y **los Sistemas de Información están siendo protegidos en base a un análisis de riesgos y proporcionalmente a los recursos de la Sociedad.** El Responsable de Seguridad es responsable del desarrollo de medidas que indiquen el estado y evolución de la protección de la información de la Sociedad. También es responsable de la coordinación de los esfuerzos necesarios para recoger los datos para soportar dichas medidas.

5.4 CUMPLIMIENTO

El Responsable de Seguridad deberá coordinar el cumplimiento de este Programa en todos y cada uno de los departamentos de la Sociedad: Auditoría Interna, Auditores Externos, Grupos de Sistemas de Información y cualquier otro agente interno o externo para minimizar la superposición de tareas y poder realizar comprobaciones con la amplitud suficiente.

5.5 COORDINACIÓN DE LA RESPUESTA A INCIDENTES

El manejo adecuado de incidentes relacionados con la protección de la información requiere, normalmente, la coordinación de especialistas de diferentes áreas, tales como Servicios Técnicos, Recursos Humanos y Legales. En el marco de este Programa de Protección, el Responsable de Seguridad se encargará de esta coordinación y de asegurar que se toman medidas, si fuera necesario, para reducir los riesgos asociados con los incidentes.

6 FUNCIONES Y RESPONSABILIDADES

6.1 DIRECCIÓN DE CAMERFIRMA

El apoyo continuo de la Dirección de CAMERFIRMA es crítico para la efectividad de esta Política de Seguridad. Las funciones y responsabilidades de la Dirección de CAMERFIRMA incluyen:

- Aceptar como suya la última responsabilidad sobre la protección de la información bajo control de CAMERFIRMA.
- Suministro de las directrices para el uso adecuado de los recursos de la información.
- Apoyo visible y compromiso con el cumplimiento de las normas y procedimientos que aseguren la protección de la información.
- Asegurar que las funciones de Propietario de la Información/Fichero, Responsable de Seguridad y Usuario están asignadas adecuadamente.
- Asegurar que el personal de la Sociedad ha sido informado y conoce esta Política y aquellas normas, directrices y procedimientos que la soportan.
- Aprobación de los sistemas de información utilizados en la Sociedad.

- Proporcionar los recursos, personal y financiación necesarios para la protección de la información;
- Reaccionar ante riesgos y vulnerabilidades identificados;
- Apoyar la investigación y solución de incidentes y pérdidas relacionados con la información de la Sociedad.

6.2 RESPONSABLE DE SEGURIDAD DE LA SOCIEDAD

La función del Responsable de Seguridad se ha establecido para servir de punto de referencia central de esta Política y del Programa de Protección de la Información.

El Responsable de Seguridad es la persona encargada de la implantación y/o mantenimiento de las medidas de protección asociadas con la información en su poder, con independencia del medio utilizado para su almacenamiento, los sistemas en los que se procesen o los métodos utilizados para su comunicación.

Sus funciones incluyen:

- Promover la implantación de las medidas de protección requeridas por:
  - La Dirección General
  - El Propietario de la Información (ver definición más adelante)
  - La legislación y los estándares de seguridad aplicables
- Investigar y promover la prueba e implantación de herramientas específicas para la Protección de la Información.
- Proporcionar los recursos y los conocimientos técnicos necesarios para hacer cumplir las medidas de protección requeridas.

6.3 FUNCIONES DEL PROPIETARIO DE LA INFORMACIÓN

Toda la información y **cada sistema de información** propiedad de Camerfirma deben tener un propietario designado. **La designación será realizada por el Responsable de Seguridad, con la aprobación de la Dirección General**.

Los propietarios de la información son responsables de:

- Clasificar la información de acuerdo con su sensibilidad como se describe más adelante,
- Autorizar accesos a su información,
- Especificar y comunicar los requisitos de seguridad al Responsable de Seguridad, incluyendo cualquier requisito adicional sobre los mínimos requeridos, como por ejemplo:
    - mantenimiento y destrucción de datos,
    - copias de seguridad y
    - recuperación ante un desastre,

- Asegurar también la existencia de una adecuada supervisión de los controles y medidas implantadas y la investigación y resolución adecuada de todas las incidencias detectadas.
- Aprobar los cambios a las aplicaciones que mantienen la información de la que son propietarios.

En los casos en que se tengan dudas sobre la aplicación de las normas, el Propietario y los Usuarios son responsables de contactar con el **Responsable de Seguridad** para la interpretación adecuada de dichas normas.

Conforme **nuevos sistemas de información** sean desarrollados o adquiridos, el Propietario de la Información es responsable de definir los requisitos de seguridad para los sistemas que gestionan su información. Estos requisitos incluyen, pero no se limitan a, control de acceso, mantenimiento y borrado de datos, copias de seguridad y parámetros de recuperación en caso de desastre.

Los **sistemas de información críticos** deben estar controlados durante todo el ciclo de vida del software, es decir, los **procedimientos de cambios a programas** deben estar autorizados y aprobados por el propietario.

El cargo del propietario debe determinarse sobre las consideraciones siguientes:

- quién dirige el departamento que genera la información;
- quién es responsable de la exactitud e integridad de la información;
- quién controla los costes de la creación, procesamiento, almacenamiento, transmisión y uso de la información;
- quién tiene el mejor conocimiento del valor de la información para el negocio;
- quién se verá afectado por una incidencia en la protección de dicha información.

6.4 FUNCIONES DE USUARIOS DE LA INFORMACIÓN

Dado que la información es muy importante y trascendental para el negocio de la Sociedad, todos los usuarios son responsables de la protección de la información a la que tienen acceso. Todos los usuarios que tengan contacto con información de la Sociedad deben familiarizarse con esta Política de Seguridad y las normas y directrices que la soportan, y aplicarlas de forma consistente en sus actividades en CAMERFIRMA.

Los usuarios de la información son responsables de:

- **Protección de los activos** de información en su poder conforme a los requerimientos de esta Política de Seguridad y del Propietario de la misma.
- **Protección física de los recursos** informáticos asignados.
- **Información de incidentes** de seguridad al Responsable de Seguridad, según lo indicado más adelante.
- **Uso de los recursos apropiado** a los fines del negocio de CAMERFIRMA.

7 CLASIFICACIÓN DE LA INFORMACIÓN

La protección de la información tiene varias dimensiones:

- ✓ confidencialidad (la sensibilidad frente a su difusión no autorizada).
- ✓ integridad (la exactitud y totalidad de la información).
- ✓ disponibilidad (posibilidad de acceso a la información cuando se necesite).

Para determinar qué medidas de protección necesitan implantarse, hay que asignar a la información una de las siguientes categorías:

- ✓ Confidencial,
- ✓ Uso Interno
- ✓ Pública

Clasificar la información como Pública no disminuye la necesidad de proteger su integridad y su disponibilidad. De hecho, la disponibilidad e integridad de la información puede llegar a ser crítica, provocando la necesidad de establecer medidas de protección adicionales, por ejemplo, al publicarla por medios interactivos.

La información crítica puede existir en cualquiera de las categorías definidas a continuación. El Propietario de la Información es responsable de identificar la información crítica para el negocio de la Sociedad y verificar que existen planes apropiados para asegurar la continuidad del negocio en caso de un desastre, natural o de cualquier otro tipo.

7.1 CONFIDENCIAL

Esta categoría engloba la información de mayor sensibilidad para Camerfirma. Las medidas para protegerla frente a difusiones (confidencialidad) y/o modificaciones no autorizadas (integridad) son más necesarias en esta categoría. Asimismo, deben existir controles de acceso a dicha información para restringir su utilización únicamente a las personas autorizadas.

7.2 USO INTERNO

Esta categoría se aplica a información menos sensible, que se pretende sea de uso interno de Camerfirma. Aunque su difusión a terceros no es recomendable ni deseada, no se espera que dicha difusión impacte seriamente en contra de Camerfirma, sus empleados, sus grupos de interés, y/o sus socios.

7.3 PÚBLICA

Esta categoría se aplica a la información que ha sido explícitamente aprobada por la Dirección de Camerfirma para mostrarse al público. Por definición, no existe difusión no autorizada de esta información ya que puede serlo sin riesgos potenciales.

8 CONTROLES CRIPTOGRÁFICOS

AC Camerfirma dispondrá de los siguientes controles criptográficos para la protección de la información clasificada como confidencial.

La protección de las claves criptográficas que permiten la emisión de certificados digitales a los clientes o a la jerarquía de entidades de certificación deben estar protegidas en un dispositivo homologado FIPS-140-2 nivel 3 y accesibles solamente mediante el concurso de al menos dos operadores.

El envió de email con información clasificada como CONFIDENCIAL o sujeta a la protección de la LOPD se realizara mediante emails cifrados. Todos los empleados dispondrán de un certificado digital y un software de envío de mensajes que permitan el envío cifrado de la información.

La información publicada en la página WEB se protegerá de la siguiente forma.
Formularios de acceso público para la solicitud de información o servicios se realizara mediante conexión segura HTTPS.

Acceso a aplicaciones y servicios internos, bien se por el personal propio de AC Camerfirma o bien por cualquier operador de la red de las autoridades de registro se realizaran mediante HTTPS con autenticación fuerte utilizando un certificado digital emitido por AC Camerfirma.

9 RESPONSABILIDAD INDIVIDUAL

La responsabilidad individual es esencial para la implantación de controles y medidas protectoras de la información. Sin la posibilidad de identificar la persona que ha cometido un error u omisión, es imposible proporcionar la información necesaria para corregir adecuadamente esa situación.

Todos los usuarios de la información de Camerfirma son responsables de su conducta cuando utilizan los sistemas informáticos de la Sociedad.

Esto se materializa mediante la asignación de identificadores personales únicos y contraseñas para acceder a los diferentes recursos. El usuario autorizado es responsable de todas las acciones realizadas utilizando su identificador personal/contraseña. Por tanto, las contraseñas individuales no deben ser compartidas o reveladas a otro usuario distinto del autorizado. Asimismo, el usuario autorizado es responsable de la renovación periódica de dicha contraseña con el fin de protegerla del conocimiento de usuarios no autorizados. Si una cuenta debe ser compartida, este hecho debe ser aprobado por el Propietario de la Información y deben implantarse otros mecanismos para mantener la responsabilidad individual.

Los usuarios de la información son responsables de proteger los Sistemas de Información que les han sido asignados físicamente, como por ejemplo, equipos personales, servidores, etc. El departamento de Informática debe proporcionar las herramientas y formación para facilitar la protección de la información, por ejemplo, salva-pantallas protegidos por contraseña, herramientas de cifrado, etc.

10 USOS PERMITIDOS

Los Sistemas de Información de Camerfirma (especialmente Internet, PC's, correo electrónico, etc.) se deberán usar exclusivamente según lo aprobado por la Dirección. No se deberán realizar operaciones que puedan poner en riesgo la información contenida en los dispositivos entregados por Camerfirma para la realización de las actividades profesionales correspondientes.

11 SUPERVISIÓN

Como una herramienta de mejora de la productividad, Camerfirma ha estimulado el uso de las comunicaciones electrónicas. Los sistemas de comunicación electrónica, y todos los mensajes generados o manipulados por los sistemas de comunicación electrónica, incluyendo copias de seguridad, son considerados propiedad de Camerfirma.

12 RESPUESTA ANTE UN INCIDENTE DE SEGURIDAD

Cualquier difusión, eliminación, destrucción, modificación o interrupción no autorizada en la disponibilidad de la información o uso inapropiado de las comunicaciones se considera un incidente de seguridad. Un fallo en las medidas de protección de la información para prevenir estas acciones, sea accidental o intencionado, se denomina error de seguridad. **Todo el personal de Camerfirma es responsable de informar de cualquier incidente de seguridad al Responsable de Seguridad, quien coordinará las actividades de respuesta.**

Se informará mediante envío de un correo electrónico a la siguiente dirección: **admin-sistemas@camerfirma.com** Indicando en el **asunto** del mismo las palabras "**incidencia de seguridad"**.

o a través de la aplicación de incidencias en **https://webcrm.camerfirma.com/incidencias/incidencias.php** indicando en el cuerpo de la incidencias que se marque como incidencia de seguridad.

En todo caso se seguirá los procesos marcados en el documento **IN-2010-10-08 GESTIÓN DE INCIDENCIAS.**

13 USO DE SOFTWARE AUTORIZADO

Es responsabilidad de cada empleado o colaborador de Camerfirma asegurar que el software adquirido por Camerfirma se utiliza de acuerdo con los términos de la licencia del mismo. Igualmente, es también su responsabilidad, asegurar que **cualquier software que se instale en equipos de Camerfirma tiene su licencia correspondiente.**

El software debe ser revisado y aprobado para su utilización antes de su uso en los equipos de Camerfirma. El proceso de aprobación es necesario para prevenir la introducción de software dañino en la red de Camerfirma. Este software dañino incluye Caballos de Troya, virus, gusanos, etc., que pueden provocar pérdida de la confidencialidad, integridad y/o disponibilidad de la información de Camerfirma. **El software de uso personal no debe instalarse en los equipos de Camerfirma sin la aprobación del responsable de seguridad.**

14 VIOLACIONES DE LA POLÍTICA DE SEGURIDAD

El cumplimiento de la Política de Seguridad de la Información es necesario para la protección de los derechos legales de Camerfirma. **Los transgresores de la misma estarán sujetos a las medidas disciplinares que considere oportunas la Dirección de Camerfirma, incluyendo el cese de la relación laboral.**

15 PREGUNTAS

La protección de la información es una prioridad para Camerfirma y requiere la cooperación de todos los empleados y colaboradores. Cualquier pregunta relacionada con la Política de Protección de la información o la aplicación de esta política debe realizarse al Responsable de Seguridad, mediante envío de la pregunta a la siguiente cuenta de correo electrónico:

admin-sistemas@camerfirma.com Indicando en el **asunto** del mismo las palabras "**incidencia de seguridad"**.

o a través de la aplicación de incidencias en https://webcrm.camerfirma.com/incidencias/incidencias.php indicando en el cuerpo de la incidencia que se trata de una incidencia de seguridad.

16 REVISIÓN Y EVALUACIÓN DE LA POLÍTICA DE SEGURIDAD

CAMERFIRMA realizará cambios en la presente política de Seguridad por los siguientes motivos:

- Cuando durante el proceso de mejora continua del sistema implantado, y tras el análisis de los diferentes registros que se generan se llegue a la conclusión de que se requiere una mejora importante en los sistemas implantados.
- Cuando se produzcan cambios importantes en las actividades de negocio de la compañía.
- Cuando se produzcan incidentes de seguridad suficientemente graves como para replantear toda la seguridad de la compañía.
- Si se producen cambios estructurales en la organización (cambios de ubicación, nuevos departamentos, etc.)

Los cambios realizados serán revisados y aprobados por la Dirección General y por el Responsable de Seguridad.

Todas estas actualizaciones quedarán reflejadas en la tabla que aparece en la segunda página del documento.

Independientemente a que se produzcan cambios en la política de seguridad de la Compañía, será necesario que se revise de forma periódica la política de seguridad con el fin de analizarla y poder valorar que se están cumpliendo los objetivos que se pretendía con la misma.

Estas revisiones se llevarán a cabo en la revisión anual de Dirección.

17 APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

Este documento, así como el resto de documentación – normas y procedimientos de seguridad de CAMERFIRMA- tienen el apoyo y la aprobación expresa por parte del Director General de CAMERFIRMA.

Alfonso Carcasona

Director General de AC Camerfirma SA.

Anexo – GLOSARIO

Colaboradores externos	Aquellas personas con acceso a información cuya propiedad o administración recae en Camerfirma, incluyendo consultores, contratistas y personal temporal.
Confidencialidad	La característica de la información de ser difundida sólo a personas y entidades autorizadas, con procesos en tiempo y forma autorizados.
Disponibilidad	La característica de la información y de los Sistemas de Información de ser accesible y utilizable de forma oportuna y adecuada.
Error de seguridad	Un fallo al proporcionar medidas adecuadas de protección de la información para prevenir su difusión, modificación o interrupción no autorizada.
Incidente de seguridad	Cualquier difusión, destrucción, eliminación, modificación no autorizada, interrupción de disponibilidad de la información o uso inapropiado de las comunicaciones electrónicas.
Información	Se aplica a cualquier almacenamiento, comunicación o recepción de conocimiento, tales como, datos, opiniones, incluyendo cifras, gráficos o narrativos, soportados en cualquier medio. Incluye, pero no se limita a, información personal, propiedad intelectual, material protegido por copyright, información financiera y contratos legales.
Información crítica	El término "Información crítica" se refiere a la información que puede provocar pérdidas o interrupciones en las funciones de la Sociedad si dicha información no está disponible. La criticidad de la información evalúa los datos en términos de su efecto sobre el funcionamiento normal de la Sociedad, sus operaciones, gestión o toma de decisiones. La criticidad de la información

	influye directamente sobre la frecuencia de realización de copias de seguridad y almacenamiento en ubicación distinta a su almacenamiento normal.
Integridad	La característica de la información de ser completa y exacta.
Propietario de la información	Empleado, nombrado por el Responsable de Seguridad, como máximo responsable de la creación y/o uso de la información.
Protección de la información	Las políticas, normas, directrices y prácticas definidas para asegurar que la información está segura frente a su difusión, modificación o destrucción no autorizada.
Responsable de Seguridad	Empleado responsable del mantenimiento de las medidas de protección de la información definidas por el propietario de la misma.
Sistema	Término general que engloba elementos de hardware, software, aspectos organizativos o administrativos a tener en cuenta para la protección de los recursos informáticos de la Sociedad.
Sistemas de Información	La recogida, procesamiento, transmisión y difusión de información conforme con procedimientos definidos, sean manuales o automáticos.
Usuario de la información	Personal con acceso a los activos de información.
Valor	La valoración monetaria asociada con un activo de información. Puede venir expresado en términos de coste del activo o de la pérdida financiera que puede sufrir la compañía si el activo es dañado o se convierte en inservible.