SISTEMA DE GESTIÓN DEL SERVICIO (SGS)

REQUISITOS GENERALES
POLÍTICA SEGURIDAD DE LA INFORMACIÓN

Dirección General de Infraestructuras y Espacios
Área de Infraestructuras, Mantenimiento y Eficiencia Energética

Título	Requisitos Generales del SGS		
Entregable	Política Seguridad de la Información		
Nombre del Fichero	DOC_IMEE_PolíticaSeguridadInformacion.doc		
Autor	Dirección IMEE		
Versión/Edición	01/01	**Fecha Versión**	01/04/2014
Aprobado por	Comisión de Garantía Interna de Calidad	**Fecha Aprobación**	01/04/2014

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	**Cargo**	**Área**
Comisión de Garantía Interna de Calidad		IMEE
Personal IMEE		IMEE
Ignacio Contreras Rubio	Director General	DGIE

0. Política de Seguridad de la Información.

Conforme al Acuerdo del Consejo de Gobierno de la Universidad, de 18 de diciembre de 2013, por el que se aprueba el Modelo de Gestión y Organización Administrativa-UPO, como concreción de la estructura y determinación del modelo de gestión administrativa y de Recursos Humanos para una actividad eficiente y sostenible de la Universidad Pablo de Olavide, de Sevilla, l**a Política de Seguridad de la Información** de los servicios prestado desde el área de Infraestructuras, Mantenimiento y Eficiencia Energética (IMEE), para el logro de la Mejora del Servicio que presta a la Comunidad Universitaria y la consecución de los mejores resultados en relación a todos los grupos de interés, se basa en la Política de Seguridad aprobada en la UPO en Resolución Rectoral de 11 de Julio de 2013.

1. Aprobación y entrada en vigor.

Resolución Rectoral de 11 de Julio de 2013, por la que se aprueba y hace pública la Política de Seguridad de la Información de la Universidad Pablo de Olavide, de Sevilla.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Este texto anula el anterior, que fue aprobado por el Rector en la sesión del Consejo de Dirección celebrada el 8 de febrero de 2011.

2. Introducción.

La Universidad Pablo de Olavide, de Sevilla depende de los sistemas de Tecnologías de Información y Comunicaciones (TIC) para alcanzar sus objetivos. 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 o confidencialidad 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 proactivamente a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, 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 mínimas de seguridad exigidas por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), 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 los incidentes para garantizar la continuidad de los servicios prestados.

La Universidad es consciente de que la seguridad de un sistema TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada, 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 los pliegos de licitación para proyectos de TIC.

La aprobación de esta Política manifiesta el interés de la Universidad Pablo de Olavide en la gestión de la seguridad de la información y en la mejora continua. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información y servicios, garantizando la integridad, disponibilidad y confidencialidad de los mismos, cumpliendo con el marco legal vigente y respetando las directrices, normas y procedimientos que oportunamente se establezcan.

La Universidad Pablo de Olavide establecerá las medidas técnicas, organizativas y de control que garanticen la consecución de estos objetivos y deberá estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del ENS.

3. Prevención.

La Universidad Pablo de Olavide, evita, o al menos intenta prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se implementan las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la Política, la Universidad:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

4. Detección.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, se monitoriza 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.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

5. Respuesta.

La Universidad Pablo de Olavide ha establecido mecanismos para responder eficazmente a los incidentes de seguridad.

Se ha designado un punto de contacto para las comunicaciones con respecto a incidentes detectados.

Se han establecido protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6. Recuperación.

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

7. Alcance.

Esta Política se aplica a todos los sistemas TIC (tanto servicios como información) y en particular a todos los sistemas enmarcados en el ámbito de la Administración Electrónica.

El alcance incluye a todos los Centros, Departamentos, áreas y unidades administrativas, órganos, entidades creadas o participadas mayoritariamente por la Universidad, Personal de Administración de Servicios, Personal Docente e Investigación y estudiantes que acceden a los sistemas de información de la Universidad Pablo de Olavide, así como organismos o empresas y profesionales colaboradores.

8. Misión de la Universidad Pablo de Olavide, de Sevilla.

Creada por la Ley andaluza 3/1997, de 1 de julio, la Universidad Pablo de Olavide, de Sevilla, nace con el objetivo prioritario de facilitar el ejercicio del derecho a la educación consagrado por el artículo 27.1 de la Constitución española de 1978.

El artículo 3 de los Estatutos de la Universidad establecen su misión, en los siguientes términos:

Como espacio educativo de formación superior, la Universidad Pablo de Olavide está al servicio de la sociedad y se define como un lugar de reflexión y pensamiento crítico comprometido con la contribución al progreso, con la enseñanza del respeto a los derechos fundamentales y libertades públicas, con el fomento de la igualdad entre mujeres y hombres, la solidaridad y los valores humanos y con la respuesta a las necesidades y problemas de la sociedad contemporánea. La Universidad procurará la más amplia proyección social de sus actividades, estableciendo al efecto cauces de colaboración y asistencia a la sociedad para contribuir y apoyar el progreso social, económico y cultural. Igualmente, fomentará y propiciará la participación de los miembros de su comunidad universitaria en actividades y proyectos de cooperación internacional y solidaridad, así como la realización de actividades e iniciativas que contribuyan al impulso de la igualdad entre hombres y mujeres, el apoyo permanente a las personas con necesidades especiales, la cultura de la paz, el desarrollo sostenible y el respeto al medio ambiente.

9. Marco Normativo.

La Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, insta a las Administraciones Públicas a la incorporación de las técnicas electrónicas, informáticas y telemáticas en las relaciones entre los ciudadanos y las administraciones públicas, optando de forma clara y específica por la tecnificación de la actuación administrativa frente a las tendencias burocráticas.

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos establece el derecho de todos los ciudadanos a relacionarse electrónicamente con las administraciones públicas.

La Comunidad autónoma de Andalucía cuenta con una Ley propia de Administración, la Ley 9/2007, de 22 de octubre, que regula la utilización de las nuevas tecnologías, y de entre sus aportaciones hay que destacar el refuerzo de los derechos de la ciudadanía ante la gestión administrativa y su derecho a la tramitación electrónica.

Estas Leyes obligan a un profundo cambio en las Administraciones Públicas, incluidas las Universidades, y a ellas hay que unir otras normas de relevancia como la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de dicha Ley, o 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, además de otras disposiciones concordantes y de desarrollo de todas las mencionadas anteriormente.

En cuanto al marco general del régimen jurídico de la Universidad Pablo de Olavide (normativa estatal, autonómica y la aprobada por la propia Universidad), las principales normas que lo configuran se encuentran publicadas en su página web www.upo.es, en el apartado Conoce la UPO, Normativa Universitaria. Entre ellas se ha de destacar la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y el Decreto 265/2011, de 2 de agosto, por el que se aprueba la modificación de los Estatutos de la Universidad Pablo de Olavide, de Sevilla, aprobados por Decreto 298/2003, de 21 de octubre.

Con respecto al marco normativo de la Administración Electrónica, en la sede electrónica de la Universidad, dentro del apartado Normativa reguladora consultable en el siguiente enlace https://upo.gob.es/normativa/, se encuentra accesible la normativa (externa e interna) de aplicación en el ámbito de la Administración Electrónica de la Universidad Pablo de Olavide.

10. Organización de la Seguridad.

El Consejo de Gobierno de la Universidad, en sesión de 28 de junio de 2010 acuerda crear una Comisión con competencias en Seguridad de TI como órgano colegiado de propuesta y seguimiento en materia de seguridad de los sistemas de información. Conforme a este acuerdo del Consejo de Gobierno se establecen las funciones de la Comisión con competencias en Seguridad de TI y sus reglas de funcionamiento. Esta Comisión a su vez tiene encomendadas las funciones específicas del Responsable General de Seguridad recogidas en el Documento de Seguridad conforme a los requisitos de la LOPD.

El Responsable de Seguridad de la Información determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

El Responsable de la Información y el Responsable del Servicio tienen como responsabilidad establecer los requisitos de la información y del servicio, respectivamente, en materia de seguridad.

Por otro lado, el Responsable del Sistema tiene como responsabilidad todas las tareas propias de la operación de los sistemas de información detalladas más adelante. El Administrador de la Seguridad del Sistema tiene como responsabilidad la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

Todas estas figuras se coordinarán entre sí en el seno de la Comisión con competencias en Seguridad de TI, donde también se resolverán los conflictos que puedan surgir en la aplicación de esta Política de Seguridad de la Información y normativas y/o procedimientos que la desarrollen.

Las responsabilidades del Responsable de Seguridad de la Información son:

• Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
• Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo o cualquier otra auditoría de seguridad que sea necesaria.
• Gestionar la formación y concienciación en materia de seguridad TI.
• Comprobar que las medidas de seguridad existentes son las adecuadas para las necesidades de la Universidad.
• Revisar y aprobar toda la documentación relacionada con la seguridad del sistema.
• Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Consejo de Dirección de la Universidad.

• Reportar al Consejo de Dirección de la Universidad sobre el estado general de la Seguridad de la Información.

Las responsabilidades del Responsable del Sistema son:

• Desarrollar y gestionar el Sistema durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
• Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
• Definir las políticas de acceso de usuarios al Sistema.
• Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
• Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
• Realizar el análisis y gestión de riesgos en el Sistema.
• Elaborar la documentación de seguridad del Sistema.
• Elaborar procedimientos operativos de seguridad.
• Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
• 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.
• Elaborar planes de mejora de la seguridad.
• Suspender el 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.

Las responsabilidades del Administrador de la Seguridad del Sistema son:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- 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.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- 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 al Responsable de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

11. Procedimiento de Designación.

El Responsable de la Seguridad de la Información, el Responsable de la Información y el Responsable del Servicio formarán parte de la Comisión con competencias en Seguridad de TI y serán designados por el Rector o Rectora, a propuesta de la Comisión con competencias en Seguridad de TI de la Universidad Pablo de Olavide.

El Responsable del Sistema será el máximo responsable del Servicio competente en Tecnologías de la Información y designará al Administrador de la Seguridad del Sistema que formará parte de la Comisión con competencias en Seguridad de TI.

12. Datos de carácter personal.

La Universidad trata datos de carácter personal. El Documento de seguridad recoge los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información de la Universidad se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

13. Control de acceso.

La Universidad Pablo de Olavide pone a disposición de sus usuarios la capacidad de acceder a sus sistemas de información y visualizar o modificar la información que procesan y almacenan.

Los permisos de acceso a las redes, sistemas y a la propia información serán otorgados mediante un proceso formal de aprobación que asegure que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones en la Universidad.

Todos los empleados y personal externo, así como entidades colaboradoras que accedan a los sistemas de información de la Universidad Pablo de Olavide, quedarán registrados y dispondrán de credenciales personales e intransferibles. Toda persona registrada que disponga de credenciales de acceso será responsable de mantener su confidencialidad y asegurar su correcto uso.

14. Gestión de Riesgos.

El análisis y gestión de los riesgos será parte esencial del proceso de seguridad de la información. Está gestión debe orientarse a mantener los riesgos en niveles aceptables, proporcionando el análisis una base de referencia para la aplicación de medidas, que serán en todo caso equilibradas y proporcionales a la naturaleza de los datos, su tratamiento y su exposición. Para el análisis y gestión de los riesgos, sin perjuicio de lo establecido por las leyes aplicables, se empleará alguna metodología reconocida internacionalmente.

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá al menos una vez al año o cuando cambien la información manejada, los servicios prestados, suceda un incidente grave de seguridad o se detecten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, la Comisión con competencias en Seguridad de TI establecerá una valoración de referencia para los diferentes tipos de información manejada y los diferentes servicios prestados. La Comisión con competencias en Seguridad de TI dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

15. Política de Seguridad de la Información.

Será misión de la Comisión con competencias en Seguridad de TI la elaboración y 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 el Rector o Rectora de la Universidad y difundida para que la conozcan todas las partes afectadas.

16. Desarrollo de la Política de Seguridad de la Información.

Este documento de la Política de Seguridad de la Información de la Universidad Pablo de Olavide, de Sevilla, conforme al ENS complementa las políticas de seguridad de la Universidad en materia de protección de datos de carácter personal.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad, que será bien aprobada por el Consejo de Gobierno o bien dictada por el Rector o Rectora, en función de su alcance, estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La Universidad Pablo de Olavide adoptará las medidas técnicas y organizativas necesarias para mantener sus sistemas de información adaptados a la normativa legal vigente, y especialmente a aquellas regulaciones legales relativas al tratamiento de los datos de carácter personal, cuyas medidas específicas de tratamiento figurarán en el correspondiente Documento de Seguridad. Estas medidas técnicas y organizativas podrán plasmarse en:

- Normativa técnica de seguridad (instrucciones y directrices de seguridad de la información), que será aprobada por el Rector o Rectora o el órgano en el que delegue, a propuesta de la Comisión con competencias en Seguridad de TI.
- Procedimientos de seguridad (conjunto de documentos que describen explícitamente y paso a paso cómo realizar una cierta actividad) y documentos formativos u orientativos (documentación de buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc.), que serán aprobado por el Responsable del Sistema, a propuesta del Administrador de la Seguridad del Sistema.

Dentro de esta Política de Seguridad se enmarca el Sistema de Gestión de la Seguridad de la Información (SGSI) de la Universidad Pablo de Olavide que se establecerá desde la Comisión con competencias en Seguridad de TI.

Con carácter periódico se realizarán auditorías que comprueben el grado de conformidad con la política y la legislación, y revisiones que determinen el grado de cumplimiento de los objetivos de seguridad establecidos y la eficacia de los controles establecidos. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles acciones de mejora, preventivas y correctivas, a realizar sobre los controles y la normativa de seguridad.

La normativa de seguridad estará disponible en la Web de la Universidad Pablo de Olavide para su consulta (véase punto 9, Marco Normativo).

17. Obligaciones del personal.

Todos los miembros de la Universidad tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad de la Comisión con competencias en Seguridad de TI disponer los medios necesarios para que la información llegue a los afectados.

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.

18. Responsabilidades en caso de incumplimiento de la normativa de seguridad de la información.

La Comisión con competencias en Seguridad de TI, en casos de incumplimiento de las obligaciones previstas en la Política de Seguridad de la Información o en su normativa e instrucciones de desarrollo, propondrá al órgano competente, la adopción de medidas preventivas y correctoras encaminadas a salvaguardar y proteger las redes y sistemas de información.

Si la Comisión entendiera que el personal, en el acceso o tratamiento de datos en el ejercicio de sus actividades profesionales, pudiera haber incurrido en un incumplimiento de la Política de Seguridad de la Información, instará por los cauces establecidos, la depuración de las responsabilidades disciplinarias a las que hubiera lugar.

El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario del personal al servicio de las Administraciones Publicas o de la propia Universidad Pablo de Olavide.

19. Terceras Partes.

Cuando la Universidad preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités o Comisiones con competencias en Seguridad de TI y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universidad 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 esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Las contrataciones y acuerdos de nivel de servicios que se establezcan con terceros incluirán cláusulas y garantías de cumplimiento de los requisitos de seguridad que exija la Universidad Pablo de Olavide y la normativa legal vigente.

Las aplicaciones que se desarrollen para la Universidad Pablo de Olavide deberán contemplar aspectos de seguridad de la información en todas las fases del ciclo de vida de desarrollo, desde la toma de requisitos hasta la realización de pruebas y el paso a producción.

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 el Responsable de la Información y el Responsable del Servicio antes de seguir adelante.

ANEXO I: Glosario

Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Autenticación. Procedimiento de comprobación de la identidad de un usuario como medida de seguridad frente a posibles operaciones fraudulentas a través de la Red. La finalidad que persigue esta medida de seguridad es servir de salvaguarda para comprobar que los usuarios con los que se está interactuando son realmente quienes dicen ser. Este proceso constituye una funcionalidad característica para una comunicación segura en la Red.

Confidencialidad. Propiedad o atributo consistente en proporcionar acceso a los sistemas de información únicamente a aquellos usuarios autorizados, en tiempo y forma determinados, y negar el acceso a terceros no autorizados.

Disponibilidad. Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran.
Documento de seguridad. Se trata de un documento elaborado por el responsable del fichero o tratamiento en el que se recogen las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

Integridad. Conjunto de medidas de seguridad que se incluyen en un sistema de información, que garantizan la exactitud de los datos transportados o almacenados, evitando su alteración, pérdida o destrucción, ya sea de forma accidental, por fallos de software o hardware, por condiciones medioambientales o bien, por intervención de terceros con fines fraudulentos.

Manual de seguridad. Se trata del documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del Sistema de Gestión de Seguridad de la Información (SGSI). Incluye la política que se define como Política de seguridad.

Medidas de seguridad. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Política de seguridad. Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que se consideran críticos.

Sistema de gestión de la seguridad de la información (SGSI). Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión

incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.