DISPOSICIONES GENERALES

UNIVERSIDAD DEL PAÍS VASCO

2239

ACUERDO de 25 de abril de 2013, del Consejo de Gobierno de la UPV/EHU, por el que se aprueba la Política de Seguridad de la Información de la Universidad del País Vasco / Euskal Herriko Unibertsitatea (UPV/EHU).

ANTECEDENTES

La UPV/EHU apoya su actividad en las tecnologías de la información y comunicación (TIC) para alcanzar sus objetivos institucionales. En consecuencia, los sistemas y recursos TIC deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, confidencialidad, integridad o conservación de la información y de los sistemas y servicios electrónicos que la sustenten.

A ello ha venido a dar respuesta el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, mediante la creación del Esquema Nacional de Seguridad (ENS), cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de los medios electrónicos que permita la adecuada protección de la información.

Más concretamente, el artículo 11 del ENS dispone que todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad de la información, cuya aprobación pertenecerá al titular del órgano correspondiente.

El objetivo de la Política de Seguridad de la Información de la UPV/EHU es, en definitiva, garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Con fecha 6 de marzo, la Comisión de Administración Electrónica informó favorablemente el borrador del documento de la Política de Seguridad de la Información de la UPV/EHU, que se presentó posteriormente, el pasado 21 de marzo de 2013, en sesión ordinaria del Consejo de Gobierno, concediéndose un plazo de hasta el 12 de abril para presentar enmiendas al mismo.

Transcurrido el plazo dado al respecto, no se ha presentado ninguna enmienda al texto presentado el pasado 21 de marzo de 2013.

Por todo ello, a propuesta del Secretario General, el Consejo de Gobierno

ACUERDA

Primero.– Aprobar la Política de Seguridad de la Información de la UPV/EHU en los términos del anexo.

Segundo.– Ordenar su publicación en el Boletín Oficial del País Vasco. La Política de Seguridad de la Información de la UPV/EHU entrará en vigor al día siguiente a su publicación.

Leioa, a 25 de abril de 2013.

El Rector,
IÑAKI GOIRIZELAIA ORDORIKA.

El Secretario General,
JOSE LUIS MARTÍN GONZÁLEZ.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UPV/EHU

Antecedentes

La información constituye uno de los activos esenciales para la prestación y gestión de gran parte de la actividad y servicios de la UPV/EHU, y por consiguiente, debe ser protegida y administrada diligentemente, garantizando la continuidad de los sistemas de información. Esta protección de la información cobra aún más fuerza, en un contexto actual, donde el uso de las tecnologías de la información y comunicación en el día a día de la acción administrativa viene acompañado de nuevos riesgos y amenazas para los sistemas de información.

La presente Política de Seguridad de la Información parte de la exigencia del cumplimiento de la legislación vigente en materia de Seguridad de la Información, integrada básicamente por el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (en adelante LAE), y desarrollado, por 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 (en adelante ENS), que tiene por objeto el establecimiento de los principios básicos y requisitos mínimos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información y la creación de las condiciones necesarias de confianza en su uso.

El ENS en su artículo 11 dispone que todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad de la información, que será aprobada por el titular del órgano correspondiente. Por tanto, el presente documento de carácter reglamentario deberá ser elevado a la decisión del Consejo de Gobierno de la UPV/EHU para su aprobación.

Asimismo, la UPV/EHU, en el marco del Plan Estratégico 2012-2017 (dentro del Eje IV «Gobernanza y Gestión») está desarrollando, impulsado por la Secretaría General y en coordinación con la Vicegerencia de las TICs, el proyecto de Implantación de la Administración Electrónica, del cual el presente documento forma parte. En este sentido, la Universidad establece la mejora en la calidad y eficiencia de su gestión como una de sus líneas estratégicas, manteniendo el compromiso firme en relación con la preservación de la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, conservación de la información y de los sistemas y servicios electrónicos que la sustenten.

Artículo 1.– Objeto y ámbito de aplicación.

La presente Política de Seguridad de la Información tiene por objeto definir y regular a todos los niveles los sistemas de información que permiten a la UPV/EHU prestar el servicio público de educación superior en los términos establecidos en el artículo 1 de sus Estatutos.

La presente Política de Seguridad de la Información se aplicará a todos los servicios, sistemas y demás recursos TIC de la UPV/EHU y/o que den soporte a sus procesos y que afecten a los diferentes activos de información sustentados en ellos.

Los recursos TIC de la UPV/EHU tienen como finalidad el apoyo a la docencia, a la investigación y a las tareas administrativas necesarias para su funcionamiento. Son recursos TIC de la Universidad todos los sistemas centrales y departamentales, estaciones de trabajo, ordenadores de puesto, impresoras y otros periféricos y dispositivos de salida, sistemas de localización, redes internas y externas, sistemas multiusuario y servicios de comunicaciones (transmisión telemática de voz, imagen, datos o documentos) y sistemas de almacenamiento que sean de su propiedad,

así como las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos.

En este sentido, no se considera un recurso TIC de la Universidad, y, por tanto, quedan fuera del ámbito de aplicación de la presente Política de Seguridad de la información, aquellos ordenadores personales financiados a título individual y no inventariados a nombre de la UPV/EHU. No obstante, en el caso de que se acceda a la red corporativa mediante dichos ordenadores personales, quedarán sujetos a las obligaciones establecidas en la presente Política de Seguridad de la Información y normas e instrucciones de desarrollo.

La Política de Seguridad de la Información se aplica también a todas aquellas personas, indistintamente del sector en el que se integren, Centros, departamentos, Institutos, estructuras, entidades, unidades o servicios, sean internos o externos, que hagan uso de los recursos de las TIC de la UPV/EHU.

Artículo 2.– Principios.

La presente Política de Seguridad de la Información se fundamenta en los siguientes principios básicos de protección que forman los pilares sobre los que se sustentan y sustentarán todas las actuaciones en materia de seguridad de la información que realice la UPV/EHU con su actividad.

a) La seguridad como proceso integral.

La seguridad de la información es el resultado de un proceso integral que depende de todos y cada uno de los elementos humanos, técnicos, materiales y organizativos que intervienen en su tratamiento.

b) Gestión de riesgos.

La gestión de la seguridad de la información está basada en la gestión de riesgos, cuyo objetivo debe ser mantener los niveles de riesgo dentro de unos niveles mínimos aceptables mediante el despliegue de las medidas de seguridad apropiadas y permanentemente actualizadas en todas las fases del ciclo de vida de las aplicaciones y servicios relacionados con el tratamiento de la información, estableciendo un equilibrio y proporcionalidad entre la naturaleza de los datos, los tratamientos realizados, los riesgos a los que estén expuestos y las medidas de seguridad aplicadas.

c) Prevención, reacción y recuperación.

La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen o no afecten gravemente a los datos que manejan los sistemas de información o los servicios que prestan.

Las medidas de reacción tendrán como objeto que los incidentes de seguridad se atajen a tiempo. Por su parte, las medidas de recuperación deben permitir la restauración de la información y los servicios de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

d) Líneas de defensa.

Se establece una estrategia de protección constituida por múltiples capas de seguridad, compuestas por medidas de naturaleza organizativa, operativa, física y lógica, dispuestas de tal forma que si una de ellas falla la seguridad en su conjunto no se vea comprometida. Asimismo, los sistemas de información deben diseñarse y configurarse de forma que garanticen la seguridad por defecto.

e) Coordinación y colaboración.

Las y los responsables de seguridad de la información actuarán de manera coordinada en la aplicación y control de las medidas de seguridad de la información. Esta coordinación se extenderá a todas las iniciativas y actuaciones de la UPV/EHU.

f) Reevaluación periódica y mejora continua.

La gestión de la seguridad de la información requiere una reevaluación, actualización y monitorización continua, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

g) Clasificación de la información.

La UPV/EHU clasificará e inventariará los activos de la información en virtud de su naturaleza, identificando las y los responsables de la información de acuerdo con lo establecido en la presente Política de Seguridad de la Información. El nivel de protección y las medidas a aplicar se basarán en el resultado de dicha clasificación.

Artículo 3.– Funciones y responsabilidades.

Para promover la aplicación de esta Política de Seguridad de la Información de la UPV/EHU y demás normativa e instrucciones de seguridad de la información, se establece una estructura organizativa basada en una distribución de funciones con una asignación de responsabilidades de las mismas. El desempeño de cualquiera de las responsabilidades definidas en este documento de seguridad de la información y en el ENS vendrá determinado por el acceso a los diferentes cargos o destinos, estatutarios o no, que han quedado vinculados a ellas.

Cualquier modificación de la RPT que conlleve la supresión o modificación de alguno de los puestos vinculados a la aplicación del ENS, tendrá que incorporar obligatoriamente el puesto al que quedarán vinculadas esas funciones.

1) Comité de Seguridad de la Información.

El Comité de Seguridad de la Información es el órgano colegiado que dirige, gestiona, coordina, establece y aprueba las actuaciones en materia de seguridad de la información. Este Comité estará compuesto por:

• Responsable de la información o persona en quien delegue, que actuará como presidente o presidenta.

• Responsable de Seguridad de la Información, que actuará como secretario o secretaria.

• Una o un representante de las y los Responsables de los Servicios de la información correspondiente, en función del asunto tratado en cada caso, con un máximo de 4 Responsables de los Servicios, designadas y designados por los máximos responsables de cada una de estas áreas, de acuerdo con lo establecido en el artículo 180 de los Estatutos de la UPV/EHU.

• Una o un Responsable de los Sistemas de la Información, designado por la o el Gerente o persona en quien delegue.

Todos los servicios y unidades de la UPV/EHU estarán obligados a informar y prestar apoyo al Comité de Seguridad de la Información cuando éste así lo requiera. El Comité tiene las siguientes funciones y responsabilidades concretas:

a) Elaborar e impulsar la estrategia y nuevas líneas de trabajo en lo que respecta a la seguridad de la información.

b) Promover la mejora continua del sistema de gestión de la seguridad de la información.

c) Proponer al Consejo de Gobierno la aprobación de los reglamentos y normativas generales y, en su caso, técnicas de seguridad de la información de la UPV/EHU relacionadas con la aplicación del ENS.

d) Elaborar y hacer el seguimiento de las instrucciones técnicas de seguridad de la información como desarrollo de las normativas generales aprobadas por el Consejo de Gobierno.

e) Elaborar, revisar y hacer el seguimiento regularmente de la Política de Seguridad de la Información y demás normativas generales, proponiendo al Consejo de Gobierno las modificaciones que considere oportunas.

f) Divulgar la Política de Seguridad de la Información y normativas e instrucciones de seguridad de la información aprobadas por la UPV/EHU.

g) Interpretar y resolver los conflictos surgidos en la aplicación de la Política de Seguridad de la Información y normativas e instrucciones de seguridad de la información aprobadas por la UPV/EHU.

h) Comunicar a los órganos competentes del incumplimiento de la Política de Seguridad de la Información y normativas e instrucciones derivadas e instar, en su caso, la adopción de las medidas disciplinarias correspondientes.

i) Supervisión y aprobación de las tareas de seguimiento del ENS.

j) Investigar y analizar el registro de incidentes habidos en los sistemas de información y las medidas aplicadas en cada caso.

k) Elevar al Consejo de Gobierno su informe anual sobre la gestión de la Política de Seguridad de la Información en la que podrá incluir una exposición detallada de los incidentes habidos en materia de seguridad de la información.

2) Responsable de la Información.

La figura de la o del Responsable de la Información recaerá en la Secretaria o Secretario General de la UPV/EHU. Tiene las siguientes funciones y responsabilidades:

a) Determinar los requisitos de seguridad de la información tratada.

b) Definir para cada activo de la información contemplada en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente.

c) Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes y por su cumplimiento.

d) Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

3) Responsables de los Servicios de la Información.

Las y los Responsables de los Servicios de la Información serán quienes ostenten las jefaturas de los servicios de la UPV/EHU.

Las y los Responsables de los Servicios tendrán las siguientes funciones:

a) Determinar los requisitos de seguridad de los servicios prestados que deban ser garantizados en el tratamiento de la información.

b) Definir las necesidades de seguridad de los servicios contemplados en el análisis de riesgos las diferentes dimensiones de seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente.

c) Colaborar en el análisis de impacto de los incidentes que se puedan producir y plantear las estrategias y salvaguardas ante los mismos.

4) Responsables de los Sistemas de la Información.

La figura de las o de los Responsables de los Sistemas de la Información recaerá en las personas que ocupen las jefaturas de los servicios de las TIC. Tendrán definidas las siguientes funciones y responsabilidades:

a) Garantizar que los recursos bajo su responsabilidad permanecen bajo control.

b) Satisfacer los requisitos de seguridad de los sistemas bajo su responsabilidad.

c) Llevar a cabo los procesos de seguridad en el ámbito de su área.

d) Implementar la seguridad física y lógica dentro de su área.

e) Colaborar en las auditorias de seguridad, LOPD y gestión de riesgos.

5) Responsable de Seguridad de la Información.

La figura de la o del Responsable de Seguridad de la Información recaerá en la o en el Gerente o persona en quien delegue. Tendrá definidas las siguientes funciones y responsabilidades:

a) Determinar las medidas necesarias para satisfacer los requisitos de seguridad de la información y de los servicios y verificar que las establecidas son adecuadas en todo momento para la protección de la información manejada y los servicios prestados.

b) Determinar la categoría del sistema según el procedimiento descrito en el anexo I del ENS y las medidas de seguridad que deben aplicarse.

c) Revisar la operativa de todos los activos de la información durante su ciclo de vida.

d) Acordar, junto a las o a los Responsables de los Servicios y de los Sistemas, la suspensión del manejo de cierta información o la prestación de cierto servicio si conoce deficiencias graves de seguridad.

e) Informar a la o al Responsable de Información y a las y a los Responsables de los Servicios de las incidencias funcionales moderadas.

f) Realizar informes sobre las incidencias graves producidas para su posterior presentación en el Comité de Seguridad de la Información.

g) Impulsar o instar la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la UPV/EHU en materia de seguridad de la información.

h) Llevar a cabo el seguimiento de la Política de Seguridad de la Información de manera operativa así como de la seguridad física y lógica de los recursos TIC.

i) Proponer aquella normativa e instrucciones y directrices técnicas y sus propuestas de modificaciones que considere necesaria en materia de seguridad al Comité de Seguridad de la Información.

Artículo 4.– Marco normativo en materia de seguridad de la información.

La UPV/EHU establece un marco normativo en materia de seguridad de la información estructurado por diferentes niveles de forma que los objetivos marcados por el presente documento tengan un desarrollo específico:

1) Primer nivel: la Política de Seguridad de la Información y las normativas generales.

2) Segundo nivel: las instrucciones y directrices de seguridad de la información. Conjunto de documentos que sirven para indicar cómo se debe actuar en caso de que una cierta circunstancia no esté recogida en un procedimiento explícito.

3) Tercer nivel: los procedimientos de seguridad de la información. Conjunto de documentos que describen explícitamente y paso a paso cómo realizar una cierta actividad.

4) Cuarto nivel: documentación de buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc.

La Política de Seguridad de la Información y las normativas generales serán aprobadas por el Consejo de Gobierno de la UPV/EHU a propuesta de la Secretaría General y del Comité de Seguridad de la Información, respectivamente. Las instrucciones y directrices técnicas de seguridad de la información formadas por el segundo, tercer y cuarto nivel serán aprobadas por el Comité de Seguridad de la Información a propuesta de la o del Responsable de Seguridad de la Información en colaboración con las y los Responsables de los Servicios y de los de Sistemas.

Dichas instrucciones de seguridad de la información aprobadas por el Comité de Seguridad de la Información deberán adoptarse por Resolución del Rector o Rectora cuyo incumplimiento dará lugar a la correspondiente responsabilidad disciplinaria.

Artículo 5.– Acceso a la información.

Quienes traten información de la UPV/EHU que no sea de acceso público, deberán estar debidamente identificados y tener los privilegios de acceso a la información estrictamente necesarios para desempeñar su contenido. Es por ello que el acceso a los sistemas de información debe estar controlado y limitado exclusivamente a las personas usuarias, procesos, dispositivos y sistemas de información que estén debidamente autorizadas, de forma que el acceso quede restringido exclusivamente a las funciones permitidas.

Artículo 6.– Reacción de incidentes y su registro.

Ante incidentes de seguridad de la información, las y los usuarios deberán ajustar su actuación a las instrucciones marcadas por el Protocolo de Incidentes cuya aprobación corresponderá al Comité de Seguridad de la Información de acuerdo con lo previsto en la presente Política de Seguridad de la Información. Quedará constancia en un registro de incidentes establecido al efecto, de todos los incidentes de seguridad de la información que se produzcan y las acciones de tratamiento que se sigan para su salvaguarda. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 7.– Relación con tercera partes.

Cuando la UPV/EHU preste servicios o ceda información a otras Administraciones Públicas u organismos, o accedan a información universitaria, se les hará partícipe de esta Política de Seguridad de la Información y de las normas e instrucciones derivadas, se establecerán canales de comunicación y coordinación entre los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad de la información.

Asimismo, cuando la UPV/EHU utilice servicios de terceros o ceda información a terceros, o accedan a información universitaria, se les hará igualmente partícipe de esta Política de Seguridad de la Información y de la normativa e instrucciones de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones y medidas de seguridad establecidas en dicha normativa e instrucciones, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de detección y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad de la información, al menos al mismo nivel que el establecido en esta Política de Seguridad de la Información.

En concreto, los terceros deberán garantizar el cumplimiento de políticas de seguridad de la información basadas en estándares auditables y someterse a controles y revisiones de terceros que certifiquen el cumplimiento de estas políticas. Asimismo, se garantizará mediante auditoría o certificado de destrucción/borrado que el tercero cancela y elimina los datos pertenecientes a la UPV/EHU a la finalización del contrato.

Cuando algún aspecto de la Política de la Seguridad de la Información no pueda ser satisfecho por una tercera parte, se requerirá un informe de la o del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por la o el Responsable de la Información y de los Servicios afectados antes de seguir adelante.

Artículo 8.– Obligaciones y deberes del personal.

Lo previsto en la Política de Seguridad de la Información de la UPV/EHU y demás normativa e instrucciones en materia de seguridad de la información, constituye un mandato de estricta observancia cuyo incumplimiento dará lugar a la correspondiente responsabilidad disciplinaria. A tales efectos, la UPV/EHU se compromete a formar y sensibilizar a todas y todos los miembros de la comunidad universitaria, así como a disponer los medios necesarios para que la información llegue a las personas afectadas.

Artículo 9.– Responsabilidades en caso de incumplimiento de la normativa de seguridad de la información.

El Comité de Seguridad de la Información podrá apreciar si por parte del personal que tiene acceso a datos de la UPV/EHU, o trata dichos datos en el ejercicio de sus actividades profesionales, existe algún tipo de incumplimiento en las obligaciones previstas en la Política de Seguridad de la Información o en su normativa e instrucciones de desarrollo.

En caso de incumplimiento, se prevén medidas preventivas y correctivas encaminadas a salvaguardar y proteger las redes y sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria.

Constatado un incumplimiento de la Política de Seguridad de la Información de la UPV/EHU, instará por los cauces establecidos en los Estatutos de la UPV/EHU, 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 UPV/EHU.

DISPOSICIÓN ADICIONAL

Cuando un sistema al que afecte el Esquema Nacional de Seguridad maneje datos de carácter personal, le será de aplicación lo dispuesto en la LOPD y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el ENS.

DISPOSICIÓN TRANSITORIA

El Comité de Seguridad de la Información establecerá los plazos en los que se desarrollará la normativa e instrucciones técnicas derivadas de la presente Política de Seguridad de la Información.

DISPOSICIÓN DEROGATORIA

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en la presente Política de Seguridad de la Información.

DISPOSICIÓN FINAL

La presente normativa entrará en vigor al día siguiente a su publicación en el BOPV.

ANEXO I

GLOSARIO

A continuación se describen el significado de los diferentes términos más usuales pertenecientes al vocabulario de la seguridad de la información que aparecen en el presente documento, sin perjuicio de los recogidos en el anexo IV de la ENS.

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.

Análisis de riesgos: utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Categoría de un sistema: es un nivel dentro de la escala básica-media-alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Disponibilidad: propiedad o característica consistente en que las personas, entidades o procesos autorizados tiene acceso a los mismos cuando lo requieran.

Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente se seguridad: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

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.

Principios básicos de seguridad: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Proceso: conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Requisitos mínimos de seguridad: exigencias necesarias para asegurar la información y los servicios.

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Sistema de información: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.