Títol: POLÍTICA DE SEGURETAT DE LA INFORMACIÓ DE LA UNIVERSITAT D´ALACANT.
Categoria: DISPOSICIONS GENERALS
Òrgan: Consell de Govern
Data d'aprovació: 28 de juny de 2013

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

1. ENTRADA EN VIGOR

Aquesta Política de Seguretat de la Informació entrarà en vigor l'endemà de la seua publicació en el BOUA, prèvia aprovació pel Consell de Govern.

2. INTRODUCCIÓ

La UNIVERSITAT D´ALACANT, d´ara endavant UA, depèn dels sistemes TI (tecnologies d´informació) per a aconseguir els seus objectius institucionals. En conseqüència, aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per a protegir-los davant de danys accidentals o deliberats que puguen afectar la disponibilitat, integritat o confidencialitat de la informació tractada o els serveis prestats.

Per això, l´objectiu de la seguretat de la informació és garantir la qualitat de la informació (confidencialitat, integritat, disponibilitat i usos previstos) i la prestació continuada dels serveis, actuant preventivament, supervisant l´activitat diària i reaccionant amb prestesa davant dels incidents.

Això implica que l´organització i el seu personal han d´aplicar les mesures mínimes de seguretat exigides per l´Esquema nacional de seguretat, (d´ara endavant ENS), com també fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per a garantir la continuïtat dels serveis prestats.

Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d´ofertes i en els plecs de licitació per a projectes de TI.

L´organització ha d´estar preparada per a prevenir, detectar, reaccionar i recuperar-se d´incidents, d´acord amb l´article 7 de l´ENS.

2.1. PREVENCIÓ

La Universitat ha d´evitar, o com a mínim prevenir en la mesura que siga possible, que la informació o els serveis es vegen perjudicats per incidents de seguretat. Per a fer-ho s´han d´implementar les mesures mínimes de seguretat determinades per l´ENS, i també qualsevol control addicional identificat a través d´una avaluació d´amenaces i riscos.

Aquests controls, a més dels rols i responsabilitats de seguretat de tot el personal, han d´estar clarament definits i documentats. Per a garantir el compliment de la política, cal que l´organització:

Autoritze els sistemes TI abans d´entrar en operació.

Titulo: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE ALICANTE
Categoría: DISPOSICIONES GENERALES
Órgano: Consejo de Gobierno
Fecha de aprobación: 28 de junio de 2013

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. ENTRADA EN VIGOR

Esta Política de Seguridad de la Información entrará en vigor al día siguiente de su publicación en el BOUA, previa aprobación por el Consejo de Gobierno.

2. INTRODUCCIÓN

La UNIVERSIDAD DE ALICANTE, en adelante UA, depende de los sistemas TI (Tecnologías de Información) para alcanzar sus objetivos institucionales. En consecuencia, 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.

Por ello, el objetivo de la seguridad de la información es garantizar la calidad de la información (confidencialidad, integridad, disponibilidad y usos previstos) y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Esto implica que la organización y su personal deben aplicar las medidas mínimas de seguridad exigidas por 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.

Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TI.

La organización debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1. PREVENCIÓN

La Universidad debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se deben implementar 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 organización debe:

- Autorizar los sistemas TI antes de entrar en operación.

Avalue regularment la seguretat, incloent-hi avaluacions dels canvis de configuració fets de manera rutinària.

Sol·licite la revisió periòdica per part de tercers amb la finalitat d´obtenir una avaluació independent.

2.2. DETECCIÓ

Atès que els serveis es poden degradar ràpidament a causa d´incidents, s´ha de monitoritzar l´operació de manera continuada per a detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència, segons estableix l´article 9 de l´ENS.

El monitoratge és especialment rellevant quan s´estableixen línies de defensa d´acord amb l´article 8 de l´ENS. S´establiran mecanismes de detecció, anàlisi i comunicació que arriben a les o als responsables regularment i en el moment en què es produeix una desviació significativa dels paràmetres que s´hagen preestablit com a normals.

2.3. RESPOSTA

És obligació de l'organització:

Establir mecanismes per a respondre eficaçment als incidents de seguretat.

Designar el punt de contacte per a les comunicacions pel que fa a incidents detectats en àrees de l´entitat o en altres organismes relacionats ambla UA.

Establir protocols per a l´intercanvi d´informació relacionada amb l´incident. Això inclou comunicacions, en els dos sentits, amb els Equips de Resposta a Emergències (CERT) reconeguts a escala nacional: Iris-CERT, CCN-CERT, etc.

2.4. RECUPERACIÓ

Per a garantir la disponibilitat dels serveis crítics, l´organització ha de desenvolupar plans de continuïtat dels sistemes TI com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

3. MISSIÓ

La Universitat d´Alacant és una institució pública, dinàmica i innovadora, amb projecció internacional i un campus de referència. La seua MISSIÓ és la formació integral dels seus estudiants i el compromís amb l´avanç i la millora de la societat, per mitjà de la creació i transmissió del coneixement i del desenvolupament cultural, científic i tecnològic.

Estretament relacionat amb el compliment d´aquesta missió, l´organització vol manifestar la necessitat d´una infraestructura TI que prevalga i fomente les operatives obertes, enfocades a la funcionalitat, connectivitat i servei a l´usuari, com a funcions prioritàries per a la consecució dels objectius estratègics i institucionals.

4. ABAST

A causa de la missió de l´entitat, reflectida en el punt 3 d'aquest document, l´organització no entén necessària l´aplicació de la present política de seguretat sobre tot el conjunt dels sistemes informàtics de

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada 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 las o los responsables regularmente y en el momento en que se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

La organización debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.

- Designar el punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con la UA.

- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT) reconocidos a nivel nacional: Iris-CERT, CCN-CERT,…

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, la organización debe desarrollar planes de continuidad de los sistemas TI como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. MISIÓN

La Universidad de Alicante es una institución pública, dinámica e innovadora, con proyección internacional y un campus de referencia, cuya MISIÓN es la formación integral de sus estudiantes y el compromiso con el avance y la mejora de la sociedad, por medio de la creación y transmisión del conocimiento y del desarrollo cultural, científico y tecnológico.

De forma estrechamente relacionada con el cumplimiento de esta misión, la organización desea manifestar la necesidad de una infraestructura TI que prime y fomente las operativas abiertas, enfocadas a la funcionalidad, conectividad y servicio al usuario, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales.

4. ALCANCE

Debido a la misión de la entidad, reflejada en el punto 3 del presente documento, la organización no considera necesaria la aplicación de la presente política de seguridad sobre todo el conjunto de los sistemas

la Universitat.

Sobre aquesta base, l´organització aplicarà la present política sobre el gruix dels sistemes TI que formen el sistema d´informació de la UA, i específicament sobre tots aquells sistemes que estan relacionats amb l´exercici de drets per mitjans electrònics, amb el compliment de deures per mitjans electrònics o al procediment administratiu.

De manera concreta, la present política de seguretat és aplicable sobre els següents serveis i els sistemes TI que els formen:

Sistema ERP Institucional

Sistema d´Administració Electrònica

Sistema Web

Sistema Serveis Universitaris

5. MARC NORMATIU

Són aplicables les lleis i normatives espanyoles en relació amb la protecció de dades personals, propietat intel·lectual i ús d´eines telemàtiques.

Aquesta política se situa dins del marc jurídic definit per les lleis i reials decrets següents:

Llei Orgànica d´universitats (6/2001) i Llei Orgànica de modificació dela LOU(4/2007)

Esquema nacional de seguretat (RD 3/2010)

Llei d´accés electrònic dels ciutadans als serveis públics (11/2007)

Llei Orgànica de protecció de dades (15/1999) i Reglament de desenvolupament dela Llei Orgànica(RD 1720/2007)

Llei de serveis de la societat de la informació (de 12 d´octubre de 2002)

6. ORGANITZACIÓ DE LA SEGURETAT

6.1. COMITÈS: FUNCIONS I RESPONSABILITATS

El Comitè de Seguretat TI estarà format per:

- El/la Vicerector/a de Tecnologies de la Informació o el/la Vicerrector/a amb competències en el tema

- El/la Secretari/a General

- El/la director/a del Secretariat de Tecnologies de la Informació

- El/la director/a del Secretariat de Serveis en Xarxa

- El/la director/a d´Àrea de Recursos de la Informació i Serveis en Xarxa

- El/la director/a del Servei d´Informàtica

informáticos de la Universidad.

En base a ello, la organización aplicará la presente política sobre el grueso de los sistemas TI que conforman el sistema de información de la UA y específicamente sobre todos aquellos que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o al procedimiento administrativo.

De forma concreta la presente política de seguridad es aplicable sobre los siguientes servicios y los sistemas TI que los conforman:

- Sistema ERP Institucional.
- Sistema de Administración Electrónica.
- Sistema Web.
- Sistema Servicios Universitarios.

5. MARCO NORMATIVO

Son de aplicación las leyes y normativas españolas en relación a protección de datos personales, propiedad intelectual y uso de herramientas telemáticas.

Esta política se sitúa dentro del marco jurídico definido por las leyes y Reales Decretos siguientes:

- Ley Orgánica de Universidades (6/2001) y Ley Orgánica de modificación de la L.O.U. (4/2007).
- Esquema Nacional de Seguridad (RD 3/2010)
- Ley de acceso electrónico de los ciudadanos a los servicios públicos (11/2007).
- Ley Orgánica de Protección de Datos (15/1999) y Reglamento de desarrollo de la Ley Orgánica (RD 1720/2007)
- Ley de Servicios de la Sociedad de la Información (de 12 de octubre de 2002)

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad TI estará formado por:

- El/la Vicerrector/a de Tecnologías de la Información o el/la Vicerrector/a competente en la materia

- El/la Secretario/a General

- El/la director/a del Secretariado de Tecnologías de la Información

- El/la director/a del Secretariado de Servicios en Red

- El/la Jefe/a de Área de Recursos de la Información y Servicios en Red

- El/la director/a del Servicio de Informática

- El/la director/a de la Divisió de Sistemes del Servei d´Informàtica

- El/la director/a de la Divisió d´Aplicacions del Servei d´Informàtica

El Comitè de Seguretat TI nomenarà un secretari o secretària, que tindrà com a funcions les pròpies del càrrec.

El Comitè de Seguretat TI reportarà al Consell de Direcció.

El Comitè de Seguretat TI tindrà les funcions següents:

Divulgació de la política i normativa de seguretat de l´organització.

Aprovació de la normativa de seguretat de l´organització.

Revisió anual de la política de seguretat.

Desenvolupament del procediment de designació de rols.

Designació de rols i responsabilitats.

Supervisió i aprovació de les tasques de seguiment de l´Esquema nacional de seguretat:

Tasques d´adequació

Anàlisi de riscos

Auditoria biennal

6.2. ROLS: FUNCIONS I RESPONSABILITATS

Responsable dels serveis TI

El/la vicerector/a de TI tindrà el rol de responsable dels serveis TI de l´organització. Les seues funcions seran:

Establiment dels requisits dels serveis TI en matèria de seguretat.

Treball en col·laboració amb la persona responsable de seguretat i la persona responsable de sistemes en el manteniment dels sistemes catalogats segons l´annex I de l´Esquema nacional de seguretat.

Responsable de la informació

La Direcció d´Àrea de Recursos de la Informació i Serveis en Xarxa tindrà el rol de responsable de la informació de l´organització. Tindrà les funcions següents:

Establiment dels requisits de la informació en matèria de seguretat.

Treball en col·laboració amb el responsable de seguretat i el de sistema en el manteniment dels sistemes catalogats segons l´annex I de l´Esquema nacional de seguretat.

Responsable de seguretat

- El/la Jefe/a de la División de Sistemas del Servicio de Informática

- El/la Jefe/a de la División de Aplicaciones del Servicio de Informática

El Comité de Seguridad TI nombrará un secretario o secretaria, que tendrá como funciones las propias del cargo.

El Comité de Seguridad TI reportará al Consejo de Dirección.

El Comité de Seguridad TI tendrá las siguientes funciones:

- Divulgación de la política y normativa de seguridad de la Organización.
- Aprobación de la normativa de seguridad de la Organización.
- Revisión anual de la política de seguridad.
- Desarrollo del procedimiento de designación de roles.
- Designación de roles y responsabilidades.
- Supervisión y aprobación de las tareas de seguimiento del Esquema Nacional de Seguridad:
- Tareas de adecuación
- Análisis de Riesgos
- Auditoría Bienal

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Responsable de los servicios TI

El/la Vicerrector/a de TI tendrá el rol de responsable de los servicios TI de la Organización. Teniendo por funciones las siguientes:

- Establecimiento de los requisitos de los servicios TI en materia de seguridad.
- Trabajo en colaboración con el/la responsable de seguridad y el/la de sistemas en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

Responsable de la información

El/la Jefe/a de Área de Recursos de la Información y Servicios en Red tendrá el rol de responsable de la información de la Organización. Teniendo por funciones las siguientes:

- Establecimiento de los requisitos de la información en materia de seguridad.
- Trabajo en colaboración con la persona responsable de seguridad y la persona responsable de sistemas en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

Responsable de Seguridad

El/la director/a del Servei d´Informàtica en el rol de responsable de seguretat de l´Organització. Té aquestes funcions:

Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes TI en el seu àmbit de responsabilitat.

Fer o promoure les auditories periòdiques que permeten verificar el compliment de les obligacions de l´organisme en matèria de seguretat.

Promoure la formació i conscienciació del Servei d´Informàtica dins del seu àmbit de responsabilitat.

Coordinar amb els diferents responsables que les mesures de seguretat establides són adequades per a la protecció de la informació utilitzada i els serveis prestats.

Analitzar, completar i aprovar tota la documentació relacionada amb la seguretat del sistema.

Monitoritzar l´estat de seguretat del sistema proporcionat per les eines de gestió d´esdeveniments de seguretat i mecanismes d´auditoria implementats en el sistema.

Donar suport a la investigació dels incidents de seguretat i supervisar-los des de la seua notificació fins a la seua resolució.

Aprovar els procediments de seguretat elaborats pel responsable del sistema.

Elaborar la normativa de seguretat de l´entitat.

Responsable del Sistema TI

Els/Les Directors/es de Divisió del Servei d´Informàtica en el rol de responsables del sistema de l´Organització. Les seues funcions, dins de les seues àrees d´actuació, són:

Desenvolupar, operar i mantenir el sistema durant tot el seu cicle de vida, de les seues especificacions, instal·lació i verificació del seu correcte funcionament.

Definir la topologia i política de gestió del sistema establint els criteris d´ús i els serveis que té disponibles.

Definir la política de connexió o desconnexió d´equips i noves persones usuàries en el sistema.

Aprovar els canvis que afecten la seguretat de la manera d´operació del sistema.

Decidir les mesures de seguretat que aplicaran els subministradors de components del sistema durant les etapes de desenvolupament, instal·lació i prova del sistema.

Implantar i controlar les mesures específiques de seguretat del sistema i assegurar-se que aquestes s´integren adequadament dins del marc general de seguretat.

Determinar la configuració autoritzada de maquinari i programari que s'utilitzarà en el sistema.

El/la Director/a del Servicio de Informática en el rol de responsable de seguridad de la Organización. Teniendo por funciones las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TI en su ámbito de responsabilidad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación del Servicio de Informática dentro de su ámbito de responsabilidad.
- Coordinar con los distintos responsables que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad 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.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Aprobación de los procedimientos de seguridad elaborados por el Responsable del sistema.
- Elaboración de la normativa de seguridad de la entidad.

Responsable del Sistema TI

Los/las Jefes/as de División del Servicio de Informática en el rol de responsables del sistema de la Organización. Teniendo por funciones, dentro de sus áreas de actuación, las siguientes:

- Desarrollar, operar y mantener el sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y nuevas personas usuarias en el sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del sistema y cerciorarse de que estas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el sistema.

Aprovar tota modificació substancial de la configuració de qualsevol element del sistema.

Dur a terme el preceptiu procés d´anàlisi i gestió de riscos en el sistema.

Determinar la categoria del sistema segons el procediment descrit en l´annex I de l´ENS i determinar les mesures de seguretat que han d´aplicar-se segons descriu l´annex II de l´ENS.

Elaborar i aprovar la documentació de seguretat del sistema.

Delimitar les responsabilitats de cada entitat involucrada en el manteniment, explotació, implantació i supervisió del sistema.

Investigar els incidents de seguretat que afecten el sistema, i si escau, comunicació a la persona responsable de seguretat o a qui aquesta determine.

Establir plans de contingència i emergència, i dur a terme exercicis freqüents perquè el personal s'hi familiaritze.

A més, la persona responsable del sistema pot acordar la suspensió del maneig d´una certa informació o la prestació d´un cert servei si és informat de deficiències greus de seguretat que puguen afectar la satisfacció dels requisits establits. Aquesta decisió ha de ser acordada amb les persones responsables de la informació afectada, el servei afectat i la persona responsable de seguretat, abans de ser executada.

Elaboració dels procediments de seguretat necessaris per a l´operativa en el sistema.

6.3. PROCEDIMENT DE DESIGNACIÓ

De conformitat amb el llocs reflectits en la política de seguretat.

6.4. POLÍTICA DE SEGURETAT

Serà missió del Comitè de Seguretat TI la revisió anual d´aquesta política de seguretat de la informació i la proposta de revisió o manteniment d'aquesta. La política serà aprovada per Consell de Govern i difosa perquè la coneguen totes les parts afectades.

7. DADES DE CARÀCTER PERSONAL

La UA fa tractaments en els quals utilitza dades de caràcter personal. El Document de seguretat LOPD de l´organització es pot trobar en les dependències del Servei d´Informàtica. Aquest document recull els fitxers afectats i les persones responsables corresponents.

Tots els sistemes d´informació de la UA s´ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal recollides en el Document de seguretat esmentat.

8. GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta política hauran de fer una

- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el sistema.
- 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.
- Elaborar y aprobar la documentación de seguridad del sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.
- Investigar los incidentes de seguridad que afecten al sistema, y en su caso, comunicación a la persona responsable de seguridad o a quien esta determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, la persona responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con las personas responsables de la información afectada, el servicio afectado y la persona responsable de seguridad, antes de ser ejecutada.
- Elaboración de los procedimientos de seguridad necesarios para la operativa en el sistema.

6.3. PROCEDIMIENTO DE DESIGNACIÓN

Acorde a los puestos reflejados en la política de seguridad.

6.4. POLÍTICA DE SEGURIDAD

Será misión del Comité de Seguridad TI 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 Consejo de Gobierno y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

La UA realiza tratamientos en los que hace uso de datos de carácter personal. El Documento de Seguridad LOPD de la Organización se puede encontrar en las dependencias del Servicio de Informática. Este documento recoge los ficheros afectados y las personas responsables correspondientes.

Todos los sistemas de información de la UA 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.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis

anàlisi de riscos per a avaluar les amenaces i els riscos als quals estan exposats. Aquesta anàlisi es repetirà:

Regularment, com a mínim una vegada cada dos anys.

Quan canvie la informació utilitzada.

Quan canvien els serveis prestats.

Quan ocórrega un incident greu de seguretat.

Quan es reporten vulnerabilitats greus.

Per a l´harmonització de les anàlisis de riscos, el Comitè de Seguretat TI establirà una valoració de referència per als diferents tipus d´informació utilitzats i els diferents serveis prestats.

El Comitè de Seguretat TI dinamitzarà la disponibilitat de recursos per a atendre les necessitats de seguretat dels diferents sistemes i promourà inversions de caràcter horitzontal.

9. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT

Aquesta política es desenvoluparà per mitjà de normativa de seguretat que aborde aspectes específics. La normativa de seguretat estarà a la disposició de qualsevol membre de l´organització que necessite conèixer-la, en particular per qui utilitzen, operen o administren els sistemes d´informació i comunicacions.

La normativa de seguretat estarà disponible en el lloc web de la Universitat.

10. OBLIGACIONS DEL PERSONAL

Totes les persones que formen part de la UA tenen l´obligació de conèixer i complir aquesta Política de seguretat de la informació i la Normativa de seguretat desenvolupada a partir d´aquesta. És responsabilitat del Comitè de Seguretat TI disposar els mitjans necessaris perquè la informació arribe a les persones o el servicis afectats.

S´establirà un programa d´accions de conscienciació contínua per a atendre a la totalitat dels y les membres de la UA, en particular a qui s'acabe d'incorporar.

Les persones amb responsabilitat en l´ús, operació o administració de sistemes TI rebran formació per a la utilització segura dels sistemes en la mesura en què la necessiten per a fer el seu treball. La formació serà obligatòria abans d´assumir una responsabilitat, tant si és la seua primera assignació o si es tracta d´un canvi de lloc de treball o canvi de responsabilitats.

11. TERCERES PARTS

Quan la UA preste serveis a altres organismes o utilitze informació d´altres organismes, se´ls farà partícips d´aquesta Política de seguretat de la informació, s´establiran canals per a la comunicació i coordinació dels respectius comitès de seguretat TI i s´establiran procediments d´actuació per a la reacció davant d'incidents de seguretat.

Quan la UA utilitze serveis de tercers o cedisca informació a tercers, se´ls exigirà el compliment d´aquesta Política de seguretat i de la

de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez cada dos años.
- 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 de Seguridad TI establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad TI dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de cualquier miembro de la organización que necesite conocerla, en particular para quienes utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en el sitio web de la Universidad.

10. OBLIGACIONES DEL PERSONAL

Todas las personas que forman parte de la UA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad TI disponer los medios necesarios para que la información llegue a las personas o servicios afectados.

Se establecerá un programa de acciones de concienciación continua para atender a la totalidad de los y las miembros de la UA, en particular a quienes se acaben de incorporar.

Las personas con responsabilidad en el uso, operación o administración de sistemas TI 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.

11. TERCERAS PARTES

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

Cuando la UA utilice servicios de terceros o ceda información a terceros, se les exigirá el cumplimento de esta Política de Seguridad y

Normativa de seguretat que concernisca aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establides en aquesta normativa, i podrà desenvolupar els seus propis procediments operatius per a satisfer-la. S´establiran procediments específics de comunicació i resolució d´incidències. Quan algun aspecte d'aquesta política no puga ser satisfet per una tercera part segons es defineix en els paràgrafs anteriors, es requerirà a la persona responsable de seguretat un informe que precise els riscos en què s´incorre i la manera de tractar-los. Es requerirà l´aprovació d´aquest informe pels responsables de la informació i els serveis afectats abans de continuar endavant.

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. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se define en los párrafos anteriores, se requerirá al/a la Responsable de Seguridad un informe 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.