Títol: POLÍTICA DE SEGURETAT DE LA INFORMACIÓ
Secció: DISPOSICIONS GENERALS
Òrgan: Consell de Govern
Data d'aprovació: dijous, 15 de desembre de 2022

Aprovat per unanimitat pel Consell de Govern de la Universitat d'Alacant en la sessió ordinària del 15 de desembre de 2022.

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Índex

Título: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
Sección: DISPOSICIONES GENERALES
Órgano: Consejo de Gobierno
Fecha de aprobación: jueves, 15 de diciembre de 2022

Aprobado por unanimidad por el Consejo de Gobierno de la Universidad de Alicante en la sesión ordinaria del 15 de diciembre de 2022.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Índice

14. Terceres parts

15. Millora contínua

16. Modificacions

17. Aprovació i entrada en vigor

1. Introducció

La Universitat d'Alacant (d'ara en avant, UA) depèn dels sistemes TI (Tecnologies de la Informació) per a aconseguir els seus objectius. Aquests sistemes han de ser administrats amb diligència, i cal prendre les mesures adequades per a protegir-los de danys accidentals o deliberats que puguen afectar la seguretat de la informació tractada o els serveis prestats i estant sempre protegits contra les amenaces o els incidents amb potencial per a incidir en la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de la informació tractada i els serveis prestats.

Per a fer front a aquestes amenaces, es requereix una estratègia que s'adapte als canvis en les condicions de l'entorn per a garantir la prestació contínua dels serveis. 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), així com fer un seguiment continu dels nivells de prestació dels serveis, monitorar i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als ciberincidents per a garantir la continuïtat dels serveis prestats.

D'aquesta manera, totes les unitats administratives de la Universitat tenen present que la seguretat TI és una part integral de cada etapa del cicle de vida del sistema, des de la concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. 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 plecs de licitació per a projectes de TI.

Per tant, per a la Universitat d'Alacant, l'objectiu de la Seguretat de la Informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuar preventivament, supervisar l'activitat diària per a detectar qualsevol incident i reaccionar amb prestesa als incidents per a recuperar els serveis al més prompte possible, segons el que estableix l'article 8 de l'ENS, amb l'aplicació de les mesures que es relacionen a continuació.

1.1 Prevenció

Perquè la informació i/o els serveis no es vegen perjudicats per incidents de seguretat, la Universitat d'Alacant, ha d'implementar les mesures de seguretat establides per l'ENS, com també qualsevol altre control addicional que haja identificat com a necessari a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i les responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per a garantir el compliment de la política, la Universitat d'Alacant cal que:

· Autoritze els sistemes abans d'entrar en operació.

· Avalue regularment la seguretat, incloent l'anàlisi 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.

1.2 Detecció

14. Terceras partes

15. Mejora continua

16. Modificaciones

17. Aprobación y entrada en vigor

1. Introducción

La Universidad de Alicante (en adelante, UA) depende de los sistemas TI (Tecnologías de la Información) 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 seguridad de la información tratada o los servicios prestados y estando siempre protegidos contra las amenazas o los incidentes con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y los servicios prestados.

Para hacer frente a 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 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 los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los ciberincidentes para garantizar la continuidad de los servicios prestados.

De este modo, todas las unidades administrativas de la universidad tienen presente que la seguridad TI es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TI.

Por tanto, para la Universidad de Alicante, 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 para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, según lo establecido en el artículo 8 del ENS, con la aplicación de las medidas que se relacionan a continuación.

1.1 Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la Universidad de Alicante, debe implementar las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional que haya identificado como necesario 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 de Alicante debe:

· Autorizar los sistemas antes de entrar en operación.

· Evaluar regularmente la seguridad, incluyendo el análisis 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.

1.2 Detección

La Universitat d'Alacant, estableix controls d'operació dels sistemes d'informació amb l'objectiu de detectar anomalies en la prestació dels serveis i actuar en conseqüència segons el que disposa l'article 10 de l'ENS (reavaluació periòdica). Quan es produeix una desviació significativa dels paràmetres que s'hagen preestablit com a normals (d'acord amb l'indicat en l'article 9 de l'ENS, Línies de defensa), s'establiran els mecanismes de detecció, anàlisi i report necessaris perquè arriben als responsables regularment.

1.3 Resposta

La Universitat d'Alacant, ha d'establir les mesures següents:

· Mecanismes per a respondre eficaçment als incidents de seguretat.

· Designar un punt de contacte per a les comunicacions respecte a incidents detectats en altres departaments o en altres organismes.

· 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)

1.4 Recuperació

Per a garantir la disponibilitat dels serveis, la Universitat d'Alacant, ha de disposar dels mitjans i tècniques necessàries que permeten garantir la recuperació dels serveis més crítics.

2. Missió de la Universitat d'Alacant

La Universitat d'Alacant té com a missió essencial procurar una formació integral dels seus estudiants, potenciar una investigació científica capdavantera i promoure la seua transferència eficaç al nostre entorn econòmic i social.

De forma estretament relacionada amb el compliment d'aquesta missió, la Universitat d'Alacant posa a la disposició de la ciutadania la realització de tràmits en línia i noves vies de participació que garantisquen el desenvolupament i l'eficàcia de les funcions i comeses. En potenciar l'ús de les noves tecnologies a la UA, es persegueix fomentar la relació electrònica tots els actors (docents, estudiants, personal investigador, personal d'administració i serveis, i uns altres) amb la universitat.

3. Principis bàsics

Els principis bàsics són directrius fonamentals de seguretat que han de tenir-se sempre presents en qualsevol activitat relacionada amb l'ús dels actius d'informació. S'estableixen els següents:

· Abast estratègic: La seguretat de la informació ha de comptar amb el compromís i el suport de tots els nivells directius de la Universitat, de manera que puga estar coordinada i integrada amb la resta d'iniciatives estratègiques de l'organització per a formar un tot coherent i eficaç.

· Responsabilitat determinada: En els sistemes TI es determinarà:

- Responsable de la Informació, que determina els requisits de seguretat de la informació tractada;
- Responsable del Servei, que determina els requisits de seguretat dels serveis prestats;
- Responsable del Sistema, que té la responsabilitat sobre la prestació dels serveis
- Responsable de la Seguretat, que determina les decisions per a satisfer els requisits de seguretat.

La Universidad de Alicante, establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el artículo 10 del ENS (reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

1.3 Respuesta

La Universidad de Alicante, debe establecer las siguientes medidas:

· Mecanismos para responder eficazmente a los incidentes de seguridad.

· Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

· 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)

1.4 Recuperación

Para garantizar la disponibilidad de los servicios, la Universidad de Alicante, debe disponer de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

2. Misión de la Universidad de Alicante

La Universidad de Alicante tiene como misión esencial procurar una formación integral de sus estudiantes, potenciar una investigación científica puntera y promover su transferencia eficaz a nuestro entorno económico y social.

De forma estrechamente relacionada con el cumplimiento de esta misión, la Universidad de Alicante pone a disposición de la ciudadanía la realización de trámites online y nuevas vías de participación que garanticen el desarrollo y la eficacia de sus funciones y cometidos. Al potenciar el uso de las nuevas tecnologías en la UA, se persigue fomentar la relación electrónica todos los actores (docentes, estudiantes, personal investigador, personal de administración y servicios, y otros) con la universidad.

3. Principios básicos

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

· Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad, de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.

· Responsabilidad determinada: En los sistemas TI se determinará:

- Responsable de la Información, que determina los requisitos de seguridad de la información tratada;
- Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados;
- Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios
- Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

· Seguretat integral: La seguretat s'entendrà com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius, relacionats amb els sistemes TI, procurant evitar qualsevol actuació puntual o tractament conjuntural. La seguretat de la informació ha de considerar-se com a part de l'operativa habitual, estant present i aplicant-se des del disseny inicial dels sistemes TI.

· Gestió de riscos: L'anàlisi i la gestió de riscos serà part essencial del procés de seguretat. La gestió de riscos permetrà el manteniment d'un entorn controlat, que minimitzarà els riscos fins a nivells acceptables. La reducció d'aquests nivells es farà mitjançant el desplegament de mesures de seguretat, que establirà un equilibri entre la naturalesa de les dades i els tractaments, l'impacte i la probabilitat dels riscos a què estiguen exposats i l'eficàcia i el cost de les mesures de seguretat. En avaluar el risc en relació amb la seguretat de les dades, s'han de tenir en compte els riscos que es deriven del tractament de les dades personals.

· Proporcionalitat: L'establiment de mesures de protecció, detecció i recuperació haurà de ser proporcional als potencials riscos i a la criticitat i valor de la informació i dels serveis afectats.

· Millora contínua: Les mesures de seguretat es reavaluaran i actualitzaran periòdicament per a adequar-ne l'eficàcia a la constant evolució dels riscos i sistemes de protecció. La seguretat de la informació serà atesa, revisada i auditada per personal qualificat, instruït i dedicat.

· Seguretat per defecte: Els sistemes han de dissenyar-se i configurar-se de manera que garantisquen un grau suficient de seguretat per defecte.

4. Objectiu de la Seguretat de la Informació

La Universitat d'Alacant estableix com a objectius de la seguretat de la informació els següents:

· Garantir la qualitat i la protecció de la informació.

· Aconseguir la plena conscienciació de les persones respecte a la seguretat de la informació.

· Gestió d'actius d'informació: Els actius d'informació de la Universitat es trobaran inventariats i categoritzats i estaran associats a un responsable.

· Seguretat lligada a les persones: S'implantaran els mecanismes necessaris perquè qualsevol persona que accedisca, o puga accedir als actius d'informació, conega les responsabilitats i d'aquesta manera es reduïsca el risc derivat d'un ús indegut, i aconseguir la plena conscienciació respecte de la seguretat de la informació.

· Seguretat física: Els actius d'informació seran emplaçats en àrees segures, protegides per controls d'accés físics adequats al nivell de criticitat. Els sistemes i els actius d'informació que contenen aquestes àrees estaran prou protegits davant d'amenaces físiques o ambientals.

· Seguretat en la gestió de comunicacions i operacions: S'establiran els procediments necessaris per a aconseguir una adequada gestió de la seguretat, operació i actualització de les TI. La informació que es transmeta a través de xarxes de comunicacions haurà de ser adequadament protegida, tenint en compte el nivell de sensibilitat i de criticitat, mitjançant mecanismes que en garantisquen la seguretat.

· Control d'accés: Es limitarà l'accés als actius d'informació, processos i altres sistemes d'informació mitjançant la implantació dels mecanismes d'identificació, autenticació i autorització d'acord amb la criticitat de cada actiu. A més, quedarà registrada la utilització del sistema amb la finalitat d'assegurar la traçabilitat de l'accés i auditar l'ús adequat d'aquest, d'acord amb l'activitat de l'organització.

· Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TI, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TI.

· Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

· Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

· Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

· Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

4. Objetivo de la Seguridad de la Información

La Universidad de Alicante establece como objetivos de la seguridad de la información los siguientes:

· Garantizar la calidad y protección de la información.

· Lograr la plena concienciación de las personas respecto a la seguridad de la información.

· Gestión de activos de información: Los activos de información de la universidad se encontrarán inventariados y categorizados y estarán asociados a un responsable.

· Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un su uso indebido, logrando su plena concienciación respecto a la seguridad de la información.

· Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

· Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TI. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

· Control de acceso: Se limitará el acceso a los activos de información, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

· Adquisició, desenvolupament i manteniment dels sistemes d'informació: Es preveuran els aspectes de seguretat de la informació en totes les fases del cicle de vida dels sistemes d'informació, i es garantirà la seua seguretat per defecte.

· Gestió dels incidents de seguretat: S'implantaran els mecanismes apropiats per a la correcta identificació, registre i resolució dels incidents de seguretat.

· Garantir la prestació continuada dels serveis: S'implantaran els mecanismes apropiats per a assegurar la disponibilitat dels sistemes d'informació i mantenir la continuïtat dels processos de negoci, d'acord amb les necessitats de nivell de servei dels usuaris.

· Protecció de dades: S'adoptaran les mesures tècniques i organitzatives que corresponga implantar per a atendre els riscos generats pel tractament per a complir la legislació de seguretat i privacitat.

· Compliment: S'adoptaran les mesures tècniques, organitzatives i procedimentals necessàries per al compliment de la normativa legal vigent en matèria de seguretat de la informació.

5. Abast

Aquesta Política de Seguretat de la Informació s'aplicarà als sistemes d'informació de la Universitat d'Alacant relacionats amb l'exercici de les seues competències i a totes les persones amb accés autoritzat a aquests, siguen empleats públics o no i amb independència de la naturalesa de la seua relació jurídica amb la universitat. Tots aquests tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la seua Normativa de Seguretat derivada, i serà responsabilitat del Comissió de Seguretat TI disposar els mitjans necessaris perquè la informació arribe al personal afectat.

6. Marc normatiu

Són aplicables les lleis i normatives espanyoles en relació amb la protecció de dades personals, propietat intel·lectual i prestació de serveis electrònics.

Aquesta Política de Seguretat de la Informació se situa dins del marc jurídic definit per les normes següents:

· Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS)

· Resolució de 13 d'octubre del 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat d'acord amb l'Esquema Nacional de Seguretat.

· Resolució de 7 d'octubre del 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat d'Informe de l'Estat de la Seguretat.

· Resolució de 27 de març del 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció Tècnica de Seguretat d'Auditoria de la Seguretat dels Sistemes d'Informació.

· Resolució de 13 d'abril del 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció Tècnica de Seguretat de Notificació d'Incidents de Seguretat.

· Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

· Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril del 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).

· Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

· Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

· Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

· Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

· Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.

· Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

5. Alcance

Esta Política de Seguridad de la Información se aplicará a los sistemas de información de la Universidad de Alicante relacionados con el ejercicio de sus competencias y a todas las personas con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la universidad. Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comisión de Seguridad TI disponer los medios necesarios para que la información llegue al personal afectado.

6. Marco normativo

Son de aplicación las leyes y normativas españolas en relación a protección de datos personales, propiedad intelectual y prestación de servicios electrónicos.

Esta Política de Seguridad de la Información se sitúa dentro del marco jurídico definido por las siguientes normas:

· Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)

· Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

· Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

· Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

· Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

· Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

· Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

· Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

· Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.

· Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.

· Reial decret 1671/2009, de 6 de novembre, pel qual es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

· Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

· Llei 9/2014, de 9 de maig, general de telecomunicacions.

· Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local, modificada per la llei 11/1999, de 21 d'abril.

· Reial decret 1308/1992, de 23 d'octubre, pel qual es declara al Laboratori del Real Institut i Observatori de l'Armada, com a Laboratori depositari del patró nacional de Temps i Laboratori associat al Centre Espanyol de Metrologia.

· Llei 57/2003, de 16 de desembre, de mesures per a la modernització del govern local.

· Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.

· Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.

· Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el Text Refós de la Llei de propietat intel·lectual.

· Reial decret legislatiu 5/2015, de 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'estatut bàsic de l'empleat públic.

· Reial decret 1553/2005, de 23 de desembre, pel qual es regula el document nacional d'identitat i els seus certificats de signatura electrònica.

· Llei 56/2007, de 28 de desembre, de mesures d'impuls de la societat de la informació.

· Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.

· Llei 9/2017, de 8 de novembre, de contractes del sector públic, per la qual es transposen a l'ordenament jurídic espanyol les directives del parlament europeu i del consell 2014/23/UE i 2014/24/UE, de 26 de febrer del 2014.

· Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions.

· Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança en la matèria.

També formen part del marc normatiu les altres normes aplicables a l'Administració Electrònica de la Universitat d'Alacant, derivades de les anteriors i publicades en la seu electrònica compreses dins de l'àmbit d'aplicació d'aquesta Política de Seguretat de la Informació.

7. Organització de la Seguretat de la Informació

7.1 Criteris utilitzats per a l'organització de la Seguretat de la Informació

· Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

· Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

· Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

· Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

· Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

· Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.

· Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.

· Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.

· Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

· Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

· Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

· Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

· Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

· Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.

· Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

· Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

· Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

· Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en la materia.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la Universidad de Alicante, derivadas de las anteriores y publicadas en la sede electrónica comprendidas dentro del ámbito de aplicación de la presente Política de Seguridad de la Información.

7. Organización de la Seguridad de la Información

7.1 Criterios utilizados para la organización de la Seguridad de la Información

La Universitat d'Alacant, tenint en compte el que estableix l'anteriorment citat Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS) i les pautes establides en la Guia CCN-STIC-801 "Responsabilitats i Funcions en l'ENS", per a organitzar la seguretat de la informació disposa de:

· Rols de seguretat: Responsables dels Serveis, responsables de la Informació, responsable de la Seguretat (RSEG), responsable del Sistema (RSIS) i delegat/ada de Protecció de Dades (DPD).

· Òrgan consultiu i estratègic per a la presa de decisions en matèria de Seguretat de la Informació. Aquest òrgan està constituït com un òrgan col·legiat i s'anomena Comitè de Seguretat TI. Estarà presidit per una persona física que serà qui assumirà la responsabilitat formal dels seus actes.

7.2 Rols i òrgans de la Seguretat de la Informació

En la Universitat d'Alacant, en el marc de l'ENS, els rols i òrgans de la Seguretat de la Informació, seran els següents:

· Responsables de la Informació: vicerector/a de Transformació Digital (o, si escau, el vicerector/a encarregat de les Tecnologies de la Informació).

· Responsables dels Serveis: gerent o vicegerent encarregat de les TI.

· Responsable de Seguretat de la Informació: cap/a de la divisió encarregat de la Seguretat de la Informació.

· Responsable de sistema: director/a del Servei d'Informàtica

· Grup de treball per a la seguretat de la informació (GTSI):

- Responsable de la Informació
- Responsable del Servei
- Responsable de Seguretat
- Responsable de Sistemes
- Membres no permanents:

. Delegat/ada de Protecció de Dades participarà amb veu, però sense vot. Podrà participar quan en aquest s'hi tracten qüestions relacionades amb el tractament de dades de caràcter personal, així com sempre que es requerisca la seua participació

. Responsables de sistemes delegats

· Comitè de Seguretat TI (COMSEGTI):

- Presidència: vicerector/a de Transformació Digital (o, si escau, el vicerector/a encarregat de les Tecnologies de la Informació).
- Vocals:
- Membres permanents:

· Secretari/ària del COMSEGTI: secretari/ària general o delegat/a

· Gerent de la Universitat o delegat/a

· Responsable de Sistema (RSIS)

· Responsable de Seguretat de la Informació (RSEG)

· Responsable del Servei

· Responsable de la Informació

· Assessors que es consideren oportuns per als temes en qüestió. Fins i tot, podrà acudir un representant del Centre Criptològic Nacional (CCN), amb veu, però sense vot.

· Delegat/ada de Protecció de Dades.

- Membres no permanents:

La Universidad de Alicante, teniendo en cuenta lo establecido en el antedicho Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y las pautas establecidas en la Guía CCN-STIC-801 "Responsabilidades y Funciones en el ENS", para organizar la seguridad de la información dispone de:

· Roles de seguridad: Responsables de los Servicios, Responsables de la Información, Responsable de la Seguridad (RSEG), Responsable del Sistema (RSIS) y Delegado/a de Protección de Datos (DPD).

· Órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano está constituido como un órgano colegiado y se denomina Comité de Seguridad TI. Estará presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

7.2 Roles y Órganos de la Seguridad de la Información

En la Universidad de Alicante, en el marco del ENS, los roles y órganos de la Seguridad de la Información, serán los siguientes:

· Responsables de la Información: Vicerrector/a de Transformación Digital (o, en su caso, el Vicerrector/a encargado de las Tecnologías de la Información).

· Responsables de los Servicios: Gerente o Vicegerente encargado de las TI.

· Responsable de Seguridad de la Información: Jefe/a de la división encargado de la Seguridad de la Información.

· Responsable de sistema: Director/a del Servicio de Informática

· Grupo de trabajo para la seguridad de la información (GTSI):

- Responsable de la Información
- Responsable del Servicio
- Responsable de Seguridad
- Responsable de Sistemas
- Miembros no permanentes:

· Delegado/a de Protección de Datos participará con voz, pero sin voto. Podrá participar cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación

· Responsables de sistemas delegados

· Comité de Seguridad TI (COMSEGTI):

- Presidencia: Vicerrector/a de Transformación Digital (o, en su caso, el Vicerrector/a encargado de las Tecnologías de la Información) .
- Vocales:
- Miembros permanentes:

· Secretario/a del COMSEGTI: Secretario/a General o delegado/a

· Gerente de la Universidad o delegado/a

· Responsable de Sistema (RSIS)

· Responsable de Seguridad de la Información (RSEG)

· Responsable del Servicio

· Responsable de la Información

· Asesores que se consideren oportunos para los temas en cuestión, pudiendo incluso acudir un representante del Centro Criptológico Nacional (CCN), con voz, pero sin voto.

· Delegado/a de Protección de datos.

- Miembros no permanentes:

· El Comitè de Seguretat TI podrà invocar la presència en les reunions tant d'altres representants de la Universitat com d'especialistes externs, dels sectors públic, privat i/o acadèmic, la presència dels quals, per raó de la seua experiència o vinculació amb els assumptes tractats, siga necessària o aconsellable.

El delegat/ada de Protecció de Dades participarà amb veu, però sense vot en les reunions del Comitè de Seguretat TI quan en aquest s'hagen de tractar qüestions relacionades amb el tractament de dades de caràcter personal, i també sempre que es requerisca la seua participació. En tot cas, si un assumpte se sotmetera a votació, es farà constar sempre en acta l'opinió del DPD.

Podran ser convocats per la presidència del Comitè de Seguretat TI en funció dels assumptes que cal tractar responsables de sistemes delegats. Igualment, podran ser convocats representants d'unitats i serveis de la Universitat d'acord amb els temes que cal tractar, en representació dels diferents àmbits o àrees de seguretat TI de la Universitat. Cada àrea estarà representada per un vocal amb vot, sense perjudici que acudisquen diversos representants d'aquesta.

El secretari/ària del Comitè farà les convocatòries i alçarà actes de les reunions del Comitè de Seguretat TI. A les sessions del Comitè de Seguretat TI podran assistir en qualitat d'assessors les persones que, en cada cas, el president crega pertinents.

7.3 Responsabilitats dels rols associats a l'Esquema Nacional de Seguretat

7.3.1 Responsable de la Informació

Seran funcions d'aquest perfil:

· Establir i elevar per a la seua aprovació al Comitè de Seguretat TI els requisits de seguretat aplicables a la informació (nivells de seguretat de la informació) dins del marc establit en l'Annex I del RD ENS, i es podrà recaptar una proposta al RSEG i tenint en compte l'opinió del RSIS.

· Dictaminar respecte als drets d'accés a la informació.

· Acceptar els nivells de risc residual que afecten la informació.

· Posar en comunicació del RSEG qualsevol variació respecte de la informació de la qual és responsable, especialment la incorporació nova informació al seu càrrec. Traslladarà aquests canvis, al Comitè de Seguretat TI, en la pròxima reunió d'aquest.

7.3.2 Responsable dels serveis

Seran funcions d'aquest perfil:

· Establir i elevar per a la seua aprovació al Comitè de Seguretat TI els requisits de seguretat aplicables als Serveis (nivells de seguretat dels serveis), dins del marc establit en l'Annex I del RD ENS, i es podrà recaptar una proposta al RSEG i tindre en compte l'opinió del RSIS.

· Dictaminar respecte als drets d'accés als serveis.

· Acceptar els nivells de risc residual que afecten els serveis.

· Posar en comunicació del RSEG qualsevol variació respecte als Serveis dels quals siga responsable, especialment la incorporació de nous Serveis a càrrec seu. Traslladarà aquests canvis, al Comitè de Seguretat TI, en la pròxima reunió d'aquest.

7.3.3 Responsable de la Seguretat de la Informació (RSEG)

Seran funcions d'aquest perfil:

· Mantenir i verificar el nivell adequat de seguretat de la informació manejada i dels serveis electrònics prestats pels sistemes d'informació.

· Promoure la formació i la conscienciació en matèria de seguretat de la informació.

· El Comité de Seguridad TI podrá invocar la presencia en sus reuniones tanto de otros representantes de la universidad como de especialistas externos, de los sectores público, privado y/o académico, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

El Delegado/a de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad TI cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del DPD.

Podrán ser convocados por la presidencia del comité de seguridad TI en función de los asuntos a tratar responsables de sistemas delegados. Igualmente, podrán ser convocados representantes de unidades y servicios de la Universidad en función de los temas a tratar, en representación de los distintos ámbitos o áreas de seguridad TI de la universidad. Cada área estará representada por un vocal con voto, sin perjuicio de que acudan varios representantes de la misma.

El Secretario/a del Comité realizará las convocatorias y levantará actas de las reuniones del Comité de Seguridad TI. A las sesiones del Comité de Seguridad TI podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

7.3 Responsabilidades de los roles asociados al Esquema Nacional de Seguridad

7.3.1 Responsable de la Información

Serán funciones de este perfil:

· Establecer y elevar para su aprobación al Comité de Seguridad TI los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al RSEG y teniendo en cuenta la opinión del RSIS.

· Dictaminar respecto a los derechos de acceso a la información.

· Aceptar los niveles de riesgo residual que afectan a la información.

· Poner en comunicación del RSEG cualquier variación respecto a la Información de la que es responsable, especialmente la incorporación nueva Información a su cargo. Dará traslado de dichos cambios, al Comité de Seguridad TI, en su próxima reunión.

7.3.2 Responsable de los Servicios

Serán funciones de este perfil:

· Establecer y elevar para su aprobación al Comité de Seguridad TI los requisitos de seguridad aplicables a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al RSEG y teniendo en cuenta la opinión del RSIS.

· Dictaminar respecto a los derechos de acceso a los servicios.

· Aceptar los niveles de riesgo residual que afectan a los servicios.

· Poner en comunicación del RSEG cualquier variación respecto a los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios a su cargo. Dará traslado de dichos cambios, al Comité de Seguridad TI, en su próxima reunión.

7.3.3 Responsable de la Seguridad de la Información (RSEG)

Serán funciones de este perfil:

· Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.

· Promover la formación y concienciación en materia de seguridad de la información.

· Designar responsables de l'execució de l'anàlisi de riscos, de la Declaració d'Aplicabilitat, identificar mesures de seguretat, determinar configuracions necessàries, fer la documentació del sistema.

· Proporcionar assessorament per a la determinació de la Categoria del Sistema, en col·laboració amb RSIS i/o Comitè de Seguretat TI.

· Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat, i validar-los.

· Gestionar les revisions externes o internes del sistema.

· Gestionar els processos de certificació.

· Elevar al Comitè de Seguretat TI l'aprovació de canvis i altres requisits del sistema.

· Aprovar els procediments de seguretat que formen part del Mapa Normatiu (i no són competència del Comitè) i posar en coneixement al Comitè de les modificacions que s'hagen fet al llarg del període en curs.

7.3.4 Responsable del Sistema (RSIS)

Seran funcions d'aquest perfil:

· Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, i fer els procediments operatius necessaris.

· Definir la topologia i la gestió del Sistema d'Informació i establir els criteris d'ús i els serveis disponibles en aquest.

· Detenir l'accés a informació o prestació de servei si té el coneixement que aquests tenen deficiències greus de seguretat.

· Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.

· Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el responsable de seguretat i/o Comitè de Seguretat TI.

· Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat.

· Dur a terme, si escau, les funcions de l'administrador de la seguretat del sistema:

- La gestió, configuració i actualització, si escau, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat.

- La gestió de les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, que inclouen el monitoratge de l'activitat desenvolupada en el sistema i la seua correspondència amb l'autoritzat.

- Aprovar els canvis en la configuració vigent del Sistema d'Informació.

- Assegurar que els controls de seguretat establits són complits estrictament.

- Assegurar que són aplicats els procediments aprovats per a manejar el Sistema d'Informació.

- Supervisar les instal·lacions de maquinari i programari, les modificacions i millores d'aquestes per a assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.

- Monitorar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.

· Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.

· Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con RSIS y/o Comité de Seguridad TI.

· Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.

· Gestionar las revisiones externas o internas del sistema.

· Gestionar los procesos de certificación.

· Elevar al Comité de Seguridad TI la aprobación de cambios y otros requisitos del sistema.

· Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.

7.3.4 Responsable del Sistema (RSIS)

Serán funciones de este perfil:

· Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.

· Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

· Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

· Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

· Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad TI.

· Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.

· Llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.

- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.

- 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

- Informar el responsable de Seguretat de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.

- Col·laborar en la investigació i la resolució d'incidents de seguretat, des de la detecció fins a la resolució d'aquests.

A causa de la complexitat del sistema de la Universitat, els caps i caps de divisió del SI, excepte qui estiga encarregat de la Seguretat de la Informació, exerciran de responsables de sistema delegats, tindran dependència funcional directa del RSIS i seran responsables en el seu àmbit d'aquelles accions que se'ls delegue. D'igual manera, el RSIS també podrà delegar en altres funcions concretes de les responsabilitats que se li atribueixen.

7.4 Delegat/ada de Protecció de Dades (DPD)

Seran funcions d'aquest perfil:

· Informar i assessorar la Universitat d'Alacant, i el personal que se n'ocupe del tractament, de les obligacions que els incumbeixen d'acord amb la normativa vigent en matèria de Protecció de Dades.

· Supervisar el compliment del que disposa la normativa de seguretat i de les polítiques internes de la Universitat d'Alacant, en matèria de protecció de dades, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.

· Oferir l'assessorament que se li sol·licite sobre l'avaluació d'impacte relativa a la protecció de dades i en supervisarà l'aplicació.

· Cooperar amb l'Agència Espanyola de Protecció de Dades quan aquesta ho requerisca, i actuar com a punt de contacte amb aquesta per a qüestions relatives al tractament de dades.

· Exercirà les seues funcions parant atenció als riscos associats a les operacions de tractament. Per a això ha de ser capaç de:

- Recaptar informació per a determinar les activitats de tractament.

- Analitzar i comprovar la conformitat de les activitats de tractament.

- Informar, assessorar i emetre recomanacions tant a responsables com a encarregats del tractament.

- Recaptar informació per a supervisar el registre de les operacions de tractament.

- Assessorar en el principi de la protecció de dades per disseny i per defecte.

- Assessorar sobre si es duu a terme o no les avaluacions d'impacte, metodologia, salvaguardes a aplicar, etc.

- Prioritzar activitats sobre la base dels riscos.

- Assessorar la persona responsable de Tractament sobre àrees a cometre a auditories, activitats de formació que cal fer i operacions de tractament a dedicar més temps i recursos.

7.5 Grup de Treball per a la seguretat de la informació (GTSI)

Seran funcions del Grup de Treball per a la seguretat de la informació:

· Assessorar en matèria de seguretat de la informació, sempre que li siga requerit.

· Aprovar procediments, protocols i instruccions de seguretat.

· Vetlar pel compliment dels procediments, protocols i instruccions de seguretat

· Aprovació dels plans de millora de la seguretat i promoure la millora contínua en la gestió de la seguretat de la informació.

· Impulsar la formació i conscienciació en matèria de seguretat TI.

- Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

- Colaborar en la investigación y resolución de incidentes deseguridad, desde su detección hasta su resolución.

Debido a la complejidad del sistema de la Universidad, los Jefes y Jefas de División del SI, excepto quien esté encargado de la Seguridad de la Información, ejercerán de responsables de sistema delegados, tendrán dependencia funcional directa del RSIS y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, el RSIS también podrá delegar en otras funciones concretas de las responsabilidades que se le atribuyen.

7.4 Delegado/a de Protección de Datos (DPD)

Serán funciones de este perfil:

· Informar y asesorar a la Universidad de Alicante, y al personal que se ocupe del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.

· Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas de la Universidad de Alicante, en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

· Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.

· Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.

· Desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:

- Recabar información para determinar las actividades de tratamiento.

- Analizar y comprobar la conformidad de las actividades de tratamiento.

- Informar, asesorar y emitir recomendaciones tanto a responsables como a encargados del tratamiento.

- Recabar información para supervisar el registro de las operaciones de tratamiento.

- Asesorar en el principio de la protección de datos por diseño y por defecto.

- Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.

- Priorizar actividades en base a los riesgos.

- Asesorar al o la Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

7.5 Grupo de trabajo para la seguridad de la información(GTSI)

Serán funciones del Grupo de trabajo para la seguridad de la información:

· Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.

· Aprobar procedimientos, protocolos e instrucciones de seguridad.

· Velar por el cumplimiento de los procedimientos, protocolos e instrucciones de seguridad

· Aprobación de los planes de mejora de la seguridad y promover la mejora continua en la gestión de la seguridad de la información.

· Impulsar la formación y concienciación en materia de seguridad TI.

· Impulsar i desenvolupar l'adequació a l'ENS.

· Resoldre els conflictes de responsabilitat que puguen aparèixer entre els diferents responsables i/o entre diferents departaments, i elevar aquells casos en què no tinga prou autoritat per a decidir.

· Periodicitat de les reunions i adopció d'acords:

- Es reunirà, almenys, una vegada al trimestre, sense perjudici que, en atenció a les necessitats derivades del compliment de les seues finalitats i atribucions, requerisca d'una major freqüència en les reunions.

- En qualsevol cas, les reunions seran convocades pel responsable de la informació, a iniciativa seua o per majoria dels membres permanents.

- Les decisions s'adoptaran per consens dels membres permanents.

7.6 Comitè de Seguretat TI (COMSEGTI)

Seran funcions del Comitè de Seguretat TI:

· Atribucions del Comitè de Seguretat TI:

- Estar permanentment informat de la normativa que regula la certificació d'acord amb l'ENS, i incloure les seues normes d'acreditació, certificació, guies, manuals, procediments i instruccions tècniques.

- Estar permanentment informat de la relació d'Entitats de Certificació acreditades i organitzacions, públiques i privades, certificades.

- Estar permanentment informat de la relació d'esquemes de certificació de la seguretat amb els quals l'Administració Pública té establits acords de reconeixement mutu de certificats.

- Proposar directrius i recomanacions, que seran arreplegades en les corresponents actes de les reunions del Comitè, a les quals el president, haurà de donar complida resposta.

- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per a assegurar que aquests siguen consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.

- Atendre les inquietuds, en matèria de Seguretat de la Informació, de l'Administració i de les diferents àrees, i informar regularment de l'estat de la seguretat de la informació a la Direcció.

- Resoldre els conflictes de responsabilitat que puguen aparèixer entre els diferents responsables i/o entre diferents departaments, i elevar aquells casos en què no tinga prou autoritat per a decidir.

- Assessorar en matèria de seguretat de la informació, sempre que li siga requerit.

- Revisar la Política de Seguretat de la Informació prèvia aprovació per l'òrgan superior.

- Aprovar la Normativa reguladora dels drets i obligacions de les persones usuàries de serveis i recursos informàtics.

- Aprovar el Mapa de Normativa amb la llista de Normativa i Procediments de seguretat per a la implantació de l'ENS.

· Periodicitat de les reunions i adopció d'acords:

· Impulsar y desarrollar la adecuación al ENS.

· Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

· Periodicidad de las reuniones y adopción de acuerdos:

- Se reunirá, al menos, una vez al trimestre, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

- En cualquier caso, las reuniones se convocarán por el Responsable de la Información, a su iniciativa o por mayoría de sus miembros permanentes.

- Las decisiones se adoptarán por consenso de los miembros permanentes.

7.6 Comité de Seguridad TI (COMSEGTI)

Serán funciones del Comité de Seguridad TI:

· Atribuciones del Comité de Seguridad TI:

- Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.

- Estar permanentemente informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.

- Estar permanentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.

- Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su presidente, deberá dar cumplida respuesta.

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

- Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la seguridad de la información a la Dirección.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

- Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.

- Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.

- Aprobar la Normativa reguladora de los derechos y obligaciones de las personas usuarios de servicios y recursos informáticos.

- Aprobar el Mapa de Normativa con la lista de Normativa y Procedimientos de seguridad para la implantación del ENS.

· Periodicidad de las reuniones y adopción de acuerdos:

- El Comitè de Seguretat TI es reunirà, almenys, dues vegades a l'any amb caràcter semestral, sense perjudici que, en atenció a les necessitats derivades del compliment de les seues finalitats i atribucions, requerisca d'una major freqüència en les reunions.

- En qualsevol cas, les reunions es convocaran per la Presidència, a través del secretari, a iniciativa seua o per majoria dels membres permanents.

- Les decisions s'adoptaran per consens dels membres permanents.

7.7 Divisió de Seguretat TI

Dins de l'estructura de governança de la UA, la Divisió encarregada de la Seguretat de la Informació exercirà les competències relacionades amb les àrees de treball següents: adequació a l'ENS, normativa i gestió de riscos, anàlisis i millora contínua, seguretat en les interconnexions i connectivitat i altres funcions connexes o concordants.

Per al desenvolupament d'aquestes competències, es constitueix un grup de treball que estarà format per:

· Responsable de Seguretat d'Informació (RSEG).

· Les persones especialistes de seguretat (AES) de la unitat de Seguretat TI i el personal d'administració de sistemes que el RSEG determine.

Les funcions d'aquestes persones seran, entre altres, les que els puguen ser encomanades pel Comitè de Seguretat TI:

· Gestió i operativa de la seguretat del Projecte d'Adequació, Implantació i gestió de la Conformitat en l'ENS, anàlisi i gestió de riscos, explotació, normativa i manteniment.

· Redacció i presentació de propostes al Comitè de Seguretat TI. Elaborarà els aspectes relacionats amb la ciberseguretat i els debatrà en primera instància, per a ser traslladats al Comitè.

· Promoure de la millora contínua del sistema de gestió de la Seguretat de la Informació. Per a això s'encarregarà de:

- Fer (i revisar regularment) la Política de Seguretat de la Informació per al seu trasllat al Comitè de Seguretat TI per a la revisió d'aquesta i posterior aprovació de l'òrgan superior.

- Fer la normativa de Seguretat de la Informació per a l'aprovació d'aquesta pel Comitè de Seguretat TI o òrgan competent.

- Verificar els procediments de seguretat de la informació i altra documentació per a l'aprovació d'aquests.

- Fer programes de formació destinats a formar i sensibilitzar el personal en matèria de seguretat de la informació i la protecció de dades.

- Fer i aprovar els requisits de formació i qualificació del personal des del punt de vista de seguretat de la informació.

- Proposar plans de millora de la seguretat de la informació, amb la dotació pressupostària corresponent, i prioritzar les actuacions en matèria de seguretat quan els recursos siguen limitats.

- Fer un seguiment dels principals riscos residuals assumits i recomanar possibles actuacions respecte d'aquests.

- Promoure la realització de les auditories periòdiques ENS i RGPD que permeten verificar el compliment de les obligacions de la Universitat en matèria de seguretat de la informació i protecció de dades.

Periodicitat de les reunions i adopció d'acords:

- El Comité de Seguridad TI se reunirá, al menos, dos veces al año con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

- En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario, a su iniciativa o por mayoría de sus miembros permanentes.

- Las decisiones se adoptarán por consenso de los miembros permanentes.

7.7 División de Seguridad TI

Dentro de la estructura de gobernanza de la UA, la División encargada de la Seguridad de la Información ejercerá las competencias relacionadas con las siguientes áreas de trabajo: adecuación al ENS, normativa y gestión de riesgos, análisis y mejora continua, seguridad en las interconexiones y conectividad y otras funciones conexas o concordantes.

Para el desarrollo de estas competencias, se constituye un grupo de trabajo que estará compuesto por :

· Responsable de Seguridad de Información (RSEG).

· Los y las especialistas de seguridad (AES) de la unidad de Seguridad TI y el personal de administración de sistemas que el RSEG determine.

Sus funciones serán, entre otras que les puedan ser encomendadas por el Comité de Seguridad TI:

· Gestión y operativa de la seguridad del Proyecto de Adecuación, Implantación y gestión de la Conformidad en el ENS, análisis y gestión de riesgos, explotación, normativa y mantenimiento.

· Redacción y presentación de propuestas al Comité de Seguridad TI. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al Comité.

· Promover de la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:

- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su traslado al Comité de Seguridad TI para su revisión y posterior aprobación del órgano superior.

- Elaborar la normativa de Seguridad de la Información para su aprobación por el Comité de Seguridad TI u órgano competente.

- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.

- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y protección de datos.

- Elaborar y aprobar los requisitos de formación y calificación del personal desde el punto de vista de seguridad de la información.

- Proponer planes de mejora de la seguridad de la información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.

- Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.

- Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones de la universidad en materia de seguridad de la Información y protección de datos.

Periodicidad de las reuniones y adopción de acuerdos:

· La persona responsable de Seguretat convocarà les reunions de treball dels membres.

· Les propostes plantejades pel grup de treball seran sotmeses a anàlisi, debat i aprovació, si escau, per part del Comitè de Seguretat TI.

· El grup de treball es reunirà, almenys, una vegada al mes i sempre abans de les celebracions del Comitè de Seguretat TI

7.8 Centre d'Operacions de Ciberseguretat (COCS)

Sota la responsabilitat i direcció del RSEG de la Universitat, el Centre d'Operacions de Ciberseguretat (COCS) presta serveis de ciberseguretat, i desenvolupa la capacitat de vigilància i detecció d'amenaces en l'operació diària dels sistemes TI, alhora que millora la capacitat de resposta del sistema davant qualsevol atac.

Estarà format per personal de la unitat de Seguretat TI adscrita a la divisió de Seguretat de la Informació i per personal de la divisió de sistemes encarregats de gestionar dispositius i programari de protecció.

7.8.1 Funcions

El Centre d'Operacions de Ciberseguretat (COCS) durà a terme les funcions següents:

· Vigilar i monitorar la seguretat dels sistemes, i dels dispositius de defensa, ja siga mitjançant interfícies previstes o instal·lant les sondes corresponents.

· Anàlisi i correlació d'esdeveniments de seguretat i registres d'activitat dels sistemes.

· Operacions de seguretat sobre els dispositius de defensa.

· Podrà constituir un Equip de Resposta a Incidents de Seguretat: fer un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d'aquests.

· Servei d'Alerta Precoç (SAP) d'alertes de seguretat en les xarxes corporatives i en les connexions a Internet dels sistemes.

· Gestió de vulnerabilitats (anàlisi i determinació de les accions d'esmena/posat de pegats) d'aplicacions i serveis.

· Anàlisi forense digital i de seguretat.

· Servei de cibervigilància que possibilite la prospectiva sobre la ciberamenaça.

El Servei d'Informàtica haurà de coordinar-se amb la Divisió de Seguretat de la Informació en la definició i l'aplicació de les mesures de seguretat en els sistemes i infraestructures que estiguen sota la seua responsabilitat; i per l'altre, col·laborar amb el Centre d'Operacions de Ciberseguretat (COCS) en les tasques d'operativa diària.

7.9 Jerarquia en el procés de decisions i mecanismes de coordinació

7.9.1 Jerarquia en el procés de decisions

Els diferents rols de seguretat de la informació (autoritat principal i possibles persones delegades) es limiten a una jerarquia simple: el Comitè de Seguretat TI i el Grup de Treball per a la Seguretat de la Informació donen instruccions al RSEG que s'encarrega d'emplenar, tot supervisant que el personal del Servei d'Informàtica complexi les mesures de seguretat segons el que estableix la política de seguretat de la informació aprovada per a la Universitat d'Alacant. Per part seua, el DPD ha de ser sentit en tots els aspectes relacionats amb la seguretat de les dades personals i violacions de seguretat de dades personals, entenent aquestes des de la perspectiva de la confidencialitat, integritat i disponibilitat.

7.9.2 Mecanismes de coordinació

Responsable del sistema:

· Responsable de Seguridad convocará las reuniones de trabajo de sus miembros.

· Las propuestas planteadas por el grupo de trabajo serán sometidas a análisis, debate y aprobación, si procede, por parte del Comité de Seguridad TI.

· El grupo de trabajo se reunirá, al menos, una vez al mes y siempre antes de las celebraciones del Comité de Seguridad TI

7.8 Centro de Operaciones de Ciberseguridad (COCS)

Bajo la responsabilidad y dirección del RSEG de la universidad, el Centro de Operaciones de Ciberseguridad (COCS) presta servicios de ciberseguridad, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TI, a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque.

Estará compuesto por personal de la unidad de Seguridad TI adscrita a la división de Seguridad de la Información y por personal de la división de Sistemas encargados de gestionar dispositivos y software de protección.

7.8.1 Funciones

El Centro de Operaciones de Ciberseguridad (COCS) llevará a cabo las siguientes funciones:

· Vigilar y monitorizar la seguridad de los sistemas, y de los dispositivos de defensa, ya sea mediante interfaces previstas o instalando las correspondientes sondas.

· Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.

· Operaciones de seguridad sobre los dispositivos de defensa.

· Podrá constituir un Equipo de Respuesta a Incidentes de Seguridad: Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.

· Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.

· Gestión de vulnerabilidades (análisis y determinación de las acciones de subsanación/parcheado) de aplicaciones y servicios.

· Análisis forense digital y de seguridad.

· Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

El Servicio de Informática deberá coordinarse con la División de Seguridad de la Información en la definición y aplicación de las medidas de seguridad en los sistemas e infraestructuras que estén bajo su responsabilidad; y por el otro, colaborar con el Centro de Operaciones de Ciberseguridad (COCS) en las tareas de operativa diaria.

7.9 Jerarquía en el proceso de decisiones y mecanismos de coordinación

7.9.1 Jerarquía en el proceso de decisiones

Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple: el Comité de Seguridad TI y el Grupo de Trabajo para la Seguridad de la Información dan instrucciones al RSEG que se encarga de cumplimentar, supervisando que el personal del Servicio de Informática implementa las medidas de seguridad según lo establecido en la política de seguridad de la información aprobada para la Universidad de Alicante. Por su parte, el DPD debe ser oído en todos los aspectos relacionados con la seguridad de los datos personales y violaciones de seguridad de datos personales, entendiendo las mismas desde la perspectiva de la confidencialidad, integridad y disponibilidad.

7.9.2 Mecanismos de coordinación

Responsable del Sistema:

· Informa el responsable de la Informació de les incidències funcionals relatives a la informació que li competeix.

· Informa el responsable del Servei de les incidències funcionals relatives al servei que li competeix.

· Ret compte al RSEG sobre:

- Actuacions en matèria de seguretat, en particular pel que fa a decisions d'arquitectura del sistema.
- Resum consolidat dels incidents de seguretat.
- Mesures de l'eficàcia de les mesures de protecció que s'han d'implantar.

Responsable de la Seguretat:

· Informa el responsable de la Informació de les decisions i incidents en matèria de seguretat que afecten la informació que li competeix, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats.

· Informa el responsable del Servei de les decisions i incidents en matèria de seguretat que afecten el servei que li competeix, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats.

· Ret compte al Grup de Treball per a la Seguretat de la Informació i/o al Comitè de Seguretat TI:

- Resum consolidat d'actuacions en matèria de seguretat.
- Resum consolidat d'incidents relatius a la seguretat de la informació.
- Estat de la seguretat del sistema, en particular del risc residual al qual el sistema està exposat.

· Ret compte al DPD sobre els aspectes que afecten la seguretat de les dades personals.

- Violacions de seguretat de les dades personals que afecten la confidencialitat, disponibilitat i integritat de les dades personals.
- Riscos detectats i mesures correctores oportunes relacionats amb la seguretat dels tractaments de dades personals.
- Demanarà assessorament davant de noves arquitectures de seguretat, polítiques i procediments que afecten el tractament de dades personals.

7.10 Procediments de designació

La designació de les persones que assumiran aquests rols identificats en l'apartat 7.2 d'aquesta Política de Seguretat de la Informació és directa després del nomenament en el lloc associat al rol de seguretat. Aquest personal ha d'acceptar les responsabilitats i les funcions associades a aquest rol.

8. Dades personals

La Universitat d'Alacant només arreplegarà i tractarà dades personals quan siguen adequades, pertinents i no excessives i aquestes es troben en relació amb l'àmbit i les finalitats per a les quals s'hagen obtingut. D'igual manera, adoptarà les mesures d'índole tècnica i organitzatives necessàries per al compliment de la normativa de Protecció de Dades.

En aplicació del principi de responsabilitat proactiva establit en el Reglament General de Protecció de Dades, les activitats de tractament de dades de caràcter personal s'integraran en la categorització de sistemes de l'Esquema Nacional de Seguretat, i es consideraran les amenaces i els riscos associats a aquest tipus de tractaments.

· Informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.

· Informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.

· Da cuenta al RSEG:

- Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
- Resumen consolidado de los incidentes de seguridad.
- Medidas de la eficacia de las medidas de protección que se deben implantar.

Responsable de la Seguridad:

· Informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

· Informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

· Da cuenta al Grupo de trabajo para la Seguridad de la Información y/o al Comité de Seguridad TI:

- Resumen consolidado de actuaciones en materia de seguridad.
- Resumen consolidado de incidentes relativos a la seguridad de la información.
- Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

· Da cuenta al DPD sobre los aspectos que afecten a la seguridad de los datos personales.

- Violaciones de seguridad de los datos personales que afecten a la confidencialidad, disponibilidad e integridad de los datos personales.
- Riesgos detectados y medidas correctoras oportunas relacionados con la seguridad de los tratamientos de datos personales.
- Pedirá asesoramiento ante nuevas arquitecturas de seguridad, políticas y procedimientos que afecten al tratamiento de datos personales.

7.10 Procedimientos de designación

La designación de las personas que asumiran estos roles identificados en el apartado 7.2 de esta Política de Seguridad de la Información es directa tras el nombramiento en el puesto asociado al rol de seguridad. Dicho personal debe aceptar las responsabilidades y funciones asociadas a dicho rol.

8. Datos personales

La Universidad de Alicante solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

En aplicación del principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos, las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

S'aplicarà, així mateix, qualsevol altra normativa vigent en matèria de protecció de dades de caràcter personal.

La Universitat d'Alacant publicarà en la Seu Electrònica la Política de Privadesa.

9. Obligacions del personal

Totes les persones que formen part de la Universitat d'Alacant tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat desenvolupada a partir d'aquesta, i serà responsabilitat del Comitè de Seguretat TI disposar dels mitjans necessaris perquè la informació arribe a les persones o els serveis afectats.

Tot el personal de la Universitat d'Alacant, comprès dins de l'àmbit de l'ENS, atendrà les sessions de conscienciació en matèria de seguretat i protecció de dades a què siga convocat. S'establirà un programa de conscienciació contínua per a atendre tot el personal, en particular el de nova incorporació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes d'informació rebran formació per al maneig segur 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 primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

10. Gestió de riscos

Tots els sistemes afectats per aquesta Política de Seguretat de la Informació estan subjectats a una anàlisi de riscos amb l'objectiu d'avaluar les amenaces i els riscos a què estan exposats. Aquesta anàlisi es repetirà:

· Almenys una vegada a l'any.

· Quan canvien la informació i/o els serveis manejats de manera significativa.

· Quan ocórrega un incident greu de seguretat o es detecten vulnerabilitats greus.

El RSEG serà l'encarregat que es faça l'anàlisi de riscos, i també d'identificar mancances i febleses i posar-les en coneixement del Comitè de Seguretat TI.

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.

El procés de gestió de riscos comprendrà les fases següents:

· Categorització dels sistemes.

· Anàlisi de riscos.

· El Comitè de Seguretat TI farà la selecció de mesures de seguretat que calga aplicar que hauran de ser proporcionals als riscos i estar justificades

Les fases d'aquest procés es faran segons el que disposen els Annexos I i II del Reial decret 311/2022, de 3 de maig, i seguint les normes, instruccions, Guies CCN-STIC i recomanacions per a l'aplicació d'aquest elaborades pel Centre Criptològic Nacional. En particular, per a fer l'anàlisi de riscos, com a norma general s'utilitzarà una metodologia reconeguda d'anàlisi i gestió de riscos.

11. Notificació d'incidents

D'acord amb el que disposa l'article 33 del RD 311/2022, de 3 de maig, la Universitat d'Alacant, notificarà al Centre Criptològic Nacional aquells incidents que tinguen un impacte significatiu en la seguretat de la informació manejada i dels serveis prestats en relació amb la categorització de sistemes arreplegada en l'Annex I d'aquest cos legal.

12. Desenvolupament de la Política de Seguretat de la Informació

Se aplicará asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

La Universidad de Alicante publicará en la Sede Electrónica su Política de Privacidad.

9. Obligaciones del personal

Todas las personas que forman parte de la Universidad de Alicante 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.

Todo el personal de la Universidad de Alicante, comprendido dentro del ámbito del ENS, atenderá las sesiones de concienciación en materia de seguridad y protección de datos a las que sea convocado. Se establecerá un programa de concienciación continua para atender a todo el personal, en particular al de nueva incorporación.

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

10. Gestión de riesgos

Todos los sistemas afectados por la presente Política de Seguridad de la Información están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

· Al menos una vez al año.

· Cuando cambien la información y/o los servicios manejados de manera significativa.

· Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El RSEG será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad TI.

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.

El proceso de gestión de riesgos comprenderá las siguientes fases:

· Categorización de los sistemas.

· Análisis de riesgos.

· El Comité de Seguridad TI procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional. En particular, para realizar el análisis de riesgos, como norma general se utilizará una metodología reconocida de análisis y gestión de riesgos.

11. Notificación de incidentes

De conformidad con lo dispuesto en el artículo 33 del RD 311/2022, de 3 de mayo, la Universidad de Alicante, notificará al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I de dicho cuerpo legal.

12. Desarrollo de la Política de Seguridad de la Información

Aquesta Política de Seguretat de la Informació serà complementada per mitjà de normativa diversa i recomanacions de seguretat (normatives i procediments de seguretat, procediments tècnics de seguretat, informes, registres i evidències electròniques). Correspon al Comitè de Seguretat TI la seua revisió anual i/o manteniment, i proposar, si escau, millores a aquesta.

El cos normatiu sobre seguretat de la informació es desenvoluparà en tres nivells per àmbit d'aplicació, nivell de detall tècnic i obligatorietat de compliment, de manera que cada norma d'un determinat nivell de desenvolupament es fonamente en les normes de nivell superior. Aquests nivells de desenvolupament normatiu són els següents:

· Primer nivell normatiu: constituït per aquesta Política de Seguretat de la Informació, la normativa reguladora dels drets i obligacions de les persones usuàries de serveis i recursos informàtics per a tot el personal i les directrius generals de seguretat aplicables als organismes o unitats de la Universitat als quals siguen d'aplicació aquests documents.

· Segon nivell normatiu: constituït per les normes de seguretat derivades de les anteriors.

· Tercer nivell normatiu: constituït per procediments, guies i instruccions tècniques. Són documents que determinen, d'acord amb l'exposat en la Política de Seguretat de la Informació, les accions o les tasques que cal fer en l'acompliment d'un procés.

Correspon al Consell de Govern de la Universitat d'Alacant l'aprovació de la Política de Seguretat de la Informació i la Normativa reguladora dels drets i obligacions de les persones usuàries de serveis i recursos informàtics de la Universitat, i és el Comitè de Seguretat TI l'òrgan responsable de l'aprovació dels altres documents, i és també responsable de la seua difusió perquè la coneguen les parts afectades.

De la mateixa manera, aquesta Política de Seguretat de la Informació complementa la Política de Privacitat de la Universitat d'Alacant, en matèria de protecció de dades. La normativa de seguretat i, molt especialment, la Política de seguretat de la Informació i la Normativa reguladora dels drets i les obligacions de les persones usuàries de serveis i recursos informàtics, serà coneguda i estarà a la disposició de tots els membres de la Universitat, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions. Estarà disponible per a la seua consulta en la Intranet de la Universitat, en suport paper, aquesta documentació serà custodiada pel Servei d'Informàtica.

13. Resolució de conflictes

En cas de conflicte entre els diferents responsables que formen l'estructura organitzativa de la Política de Seguretat de la Informació de la Universitat d'Alacant, prevaldrà la decisió del Comitè de Seguretat TI.

14. Terceres parts

Quan la Universitat d'Alacant preste serveis a altres organismes o manege informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació. S'establiran canals per a la informació i la coordinació dels respectius Comitès de Seguretat de la Informació i s'establiran procediments d'actuació per a la reacció davant d'incidents de seguretat.

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas). Corresponde al Comité de Seguridad TI su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

· Primer nivel normativo: constituido por la presente Política de Seguridad de la Información, la Normativa reguladora de los derechos y obligaciones de las personas usuarios de servicios y recursos informáticos para todo el personal y las directrices generales de seguridad aplicables a los organismos o unidades de la universidad a los que sea de aplicación dichos documentos.

· Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores.

· Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al Consejo de Gobierno de la Universidad de Alicante la aprobación de la Política de Seguridad de la Información y la Normativa reguladora de los derechos y obligaciones de las personas usuarios de servicios y recursos informáticos de la universidad, siendo el Comité de Seguridad TI el órgano responsable de la aprobación de los restantes documentos, siendo también responsable de su difusión para que la conozcan las partes afectadas.

Del mismo modo, la presente Política de Seguridad de la Información complementa la Política de Privacidad de la Universidad de Alicante, en materia de protección de datos. La normativa de seguridad y, muy especialmente, la Política de seguridad de la Información y la Normativa reguladora de los derechos y obligaciones de las personas usuarios de servicios y recursos informáticos, será conocida y estará a disposición de todos los miembros de la universidad, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en la Intranet de la Universidad, en soporte papel, esta documentación será custodiada por el Servicio de Informática.

13. Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información de la Universidad de Alicante, prevalecerá la decisión del Comité de Seguridad TI.

14. Terceras partes

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

Quan la Universitat d'Alacant, utilitze serveis de tercers o cedisca informació a tercers, se'ls farà partícip d'aquesta Política de Seguretat de la Informació i de la normativa de seguretat que concernisca a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establides en aquesta normativa, i es podran desenvolupar els seus procediments operatius propis per a satisfer-la. S'establiran procediments específics de report i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establit en aquesta Política de Seguretat de la Informació.

Quan algun aspecte d'aquesta Política de Seguretat de la Informació no puga ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del RSEG que explique els riscos en què s'incorre i la manera de tractar-los. Es requerirà l'aprovació d'aquest informe per les persones responsables de la informació i els serveis afectats abans de seguir endavant.

15. Millora contínua

La gestió de la seguretat de la informació és un procés subjecte a actualització permanent. Els canvis en l'organització, les amenaces, les tecnologies i/o la legislació són un exemple en què es veu que és necessària una millora contínua dels sistemes. Per això, cal implantar un procés permanent que implicarà, entre altres accions:

- Revisió de la Política de Seguretat de la Informació
- Revisió dels serveis i informació i la categorització d'aquests
- Execució amb periodicitat anual de l'anàlisi de riscos
- Realització d'auditories internes o, quan escaiga, externes
- Revisió de les mesures de seguretat
- Revisió i actualització de les normes i procediments

16. Modificacions

Queden derogada la Política de Seguretat de la Informació de la Universitat d'Alacant aprovada pel Consell de Govern de la Universitat d'Alacant en la sessió del 28 de juny del 2013, i també les disposicions d'igual rang o inferior que s'oposen al que disposa aquesta Política de Seguretat de la Informació.

17. Aprovació i entrada en vigor

Aquesta Política de Seguretat de la Informació ha sigut revisada per la Comissió de Seguretat TI de la Universitat d'Alacant en la sessió del 3 de novembre del 2022 i entrarà en vigor l'endemà de la seua publicació en el BOUA, prèvia aprovació pel Consell de Govern de la UA. Aquesta Política de Seguretat de la Informació és efectiva des d'aquesta data de publicació i fins que siga reemplaçada per una nova Política de Seguretat de la Informació.

Cuando la Universidad de Alicante, utilice servicios de terceros o ceda información a terceros, se les hará participe de esta Política de Seguridad de la Información y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad de la Información.

Cuando algún aspecto de esta Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del RSEG que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los y las responsables de la información y los servicios afectados antes de seguir adelante.

15. Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas. Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

- Revisión de la Política de Seguridad de la Información.
- Revisión de los servicios e información y su categorización.
- Ejecución con periodicidad anual del análisis de riesgos.
- Realización de auditorías internas o, cuando procedan, externas.
- Revisión de las medidas de seguridad.
- Revisión y actualización de las normas y procedimientos.

16. Modificaciones

Quedan derogada la Política de Seguridad de la Información de la Universidad de Alicante aprobada por el consejo de gobierno de la Universidad de Alicante en la sesión del 28 de junio de 2013, así como las disposiciones de igual o inferior rango que se opongan a lo dispuesto en la presente Política de Seguridad de la Información.

17. Aprobación y entrada en vigor

Esta Política de Seguridad de la Información ha sido revisada por la Comisión de Seguridad TI de la Universidad de Alicante en su sesión de 3 de noviembre de 2022 y entrará en vigor al día siguiente de su publicación en el BOUA, previa aprobación por el Consejo de Gobierno de la UA. Esta Política de Seguridad de la Información es efectiva desde esta fecha de publicación y hasta que sea reemplazada por una nueva Política de Seguridad de la Información.