Universidad de Valladolid

Acuerdo del Consejo de Gobierno de la Universidad de Valladolid, de 20 de julio de 2023, por el que se aprueba la "Política de seguridad de la información de la Universidad de Valladolid" de conformidad con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del Esquema Nacional de Seguridad (en adelante, ENS) a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios. A su vez, señala en su artículo 156 al ENS como instrumento fundamental para el logro de dichos objetivos.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13, incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), ordenó en su disposición adicional primera que dichas medidas de seguridad se implanten en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del 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 (en adelante, RGPD). De otra parte, la disposición adicional primera también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales.

El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente que, en el caso de la Universidad de Valladolid, es el Consejo de Gobierno.

La Política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, en la política de seguridad deberán incluirse, como mínimo, los siguientes extremos:

a) Los objetivos o misión de la organización.

b) El marco regulatorio en el que se desarrollarán las actividades.

c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

f) Los riesgos que se derivan del tratamiento de los datos personales.

En la presente Política de seguridad de la información se detallan los principios básicos y requisitos mínimos previstos por el ENS y la forma en que estos son implementados por la Universidad de Valladolid para procurar una adecuada seguridad a la información que gestiona, en función del nivel del riesgo.

En virtud de lo anterior, a propuesta del Comité de seguridad de información y previa consulta a los representantes de los trabajadores y expertos de la Universidad de Valladolid en la materia, en ejercicio de las competencias atribuidas en el artículo 83.z) de los Estatutos de la Universidad de Valladolid, este Consejo de Gobierno,

RESUELVE:

Primero.- Aprobar la Política de seguridad de la información que se adjunta al presente acuerdo, en cumplimiento de lo dispuesto en el Esquema Nacional de Seguridad.

Segundo.- El presente acuerdo, que surtirá efectos una vez aprobado y publicado en los términos normativamente previstos, deja sin efecto la Política de seguridad de la información aprobada por el Consejo Gobierno en sesión de 15 de julio de 2016.

Universidad de Valladolid

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Aprobado por el Consejo de Gobierno en sesión de
20 de julio de 2023

ÍNDICE

1. INTRODUCCIÓN 5
   1.1. Prevención 6
   1.2. Detección 6
   1.3. Respuesta 6
   1.4. Recuperación 6
2. MISIÓN DE LA UNIVERSIDAD DE VALLADOLID 6
3. PRINCIPIOS BÁSICOS 7
4. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN 8
5. ALCANCE 9
6. MARCO NORMATIVO 9
7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 10
   7.1. Criterios utilizados para la organización de la seguridad de la información 10
   7.2. Roles y órganos de la seguridad de la información 10
   7.3. Responsabilidades de los roles asociados al Esquema Nacional de Seguridad 11
      7.3.1. Responsables de la información y de los servicios 11
      7.3.2. Responsable de seguridad de la información 12
      7.3.3. Responsable del sistema 12
   7.4. Delegado de protección de datos 13
   7.5. Comité de seguridad de la información 14
      7.5.1. Atribuciones del Comité de seguridad de la información 14
      7.5.2. Responsabilidades del Comité de seguridad de la información 15
      7.5.3. Periodicidad de las reuniones y adopción de acuerdos 15
      7.5.4. Procedimientos de designación 15
   7.6. Oficina de Seguridad de la Información (OSI) 15
      7.6.1. Periodicidad de las reuniones y adopción de acuerdos 17
   7.7. Foro de seguridad TIC de las universidades 17
8. DATOS PERSONALES 18
9. OBLIGACIONES DEL PERSONAL 18
10. GESTIÓN DE RIESGOS 18
11. NOTIFICACIÓN DE INCIDENTES 19
12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 19
13. TERCERAS PARTES 20
14. MEJORA CONTINUA 20

ANEXO I – GLOSARIO DE TËRMINOS 21

1. INTRODUCCIÓN

La profunda transformación digital emprendida por la Universidad de Valladolid sitúa a la información y a la infraestructura que la soporta en la base de su funcionamiento ordinario. Los sistemas de información, basados en las tecnologías de la información y las comunicaciones (TIC), resultan hoy en día imprescindibles para alcanzar los objetivos institucionales.

Estos sistemas deben ser administrados con diligencia, adoptando las medidas adecuadas para protegerlos frente a las amenazas que los acechan. Las políticas de seguridad, las normativas que las desarrollan y la práctica institucional deben garantizar que la información tratada y los servicios prestados cuenten con un nivel de seguridad adecuado, con el objetivo esencial de disponer de sistemas confiables, robustos y resilientes.

Todo ello implica un enfoque para la gestión de riesgos capaz de identificar las amenazas externas y las vulnerabilidades internas y de gobernar la tecnología ante cualquier eventualidad. Para conseguirlo, es necesario disponer de mecanismos ágiles de evaluación de riesgos y de planes de contingencia y respuesta que eviten o remedien los daños accidentales o deliberados que puedan afectar a la información tratada o a los servicios prestados. Debe garantizarse la seguridad de los sistemas de información en todas sus dimensiones: confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad.

La protección de la información y el adecuado uso de los sistemas que la soportan, garantizando los derechos fundamentales de las personas, es un compromiso que debe involucrar al conjunto de la comunidad universitaria a todos los niveles: personal docente e investigador, personal técnico, de gestión y de administración y servicios y estudiantado. La información con la se trabaja en cada colectivo es uno de los activos más valiosos de la universidad, por lo que mantenerla segura es una tarea que corresponde a todos.

Para hacer frente a las amenazas de los sistemas de información, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno, gestionando los riesgos, con el objetivo de garantizar la prestación continua de los servicios. Esto implica la aplicación de las medidas mínimas de seguridad establecidas por el Esquema Nacional de Seguridad (ENS) para la protección de las administraciones públicas, 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, todos los miembros de la comunidad universitaria han de tener presente que la seguridad TIC 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, vinculadas al uso cotidiano del sistema. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en los pliegos de contratación para proyectos TIC.

Por tanto, para la Universidad de Valladolid, 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 para recuperar los servicios lo antes posible, según lo establecido en el artículo 8 ENS, con la aplicación de las medidas que se relacionan a continuación.

Esta Política de seguridad sigue las indicaciones de la Guía CCN-STIC-881 de Adecuación al ENS para Universidades, del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

1.1. Prevención

Para que la información y los servicios no se vean perjudicados por incidentes de seguridad, la Universidad de Valladolid implementa 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, los roles y responsabilidades de seguridad de todo el personal están claramente definidos y documentados.

Para garantizar el cumplimiento de esta política, la Universidad de Valladolid:

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

1.2. Detección

La Universidad de Valladolid 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 ENS relativo a la vigilancia continua y reevaluación periódica. Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales, conforme a lo indicado en el artículo 9 ENS sobre la existencia de 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 Valladolid establecerá 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 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 y la resiliencia de sus sistemas de información, la Universidad de Valladolid dispone de los medios y técnicas necesarios que permiten garantizar la recuperación de los servicios esenciales.

2. MISIÓN DE LA UNIVERSIDAD DE VALLADOLID

La Universidad de Valladolid presta y garantiza el servicio público de la educación superior universitaria mediante la docencia, la investigación y la transferencia del conocimiento. En nuestra sociedad, el despliegue de sus fines estatuarios, competencias y funciones se soporta sobre un

marco de innovación constante en el uso de tecnología en un contexto de profunda transformación digital de la institución universitaria. Esta transformación pone en el centro de sus valores al ser humano y la garantía de los derechos fundamentales, así como el respeto al medioambiente y el alineamiento del esfuerzo tecnológico basado en la sostenibilidad y los valores que se desprenden de los Objetivos de Desarrollo Sostenible.

Para la eficaz prestación de sus servicios, la Universidad de Valladolid pone a disposición de la ciudadanía la realización de trámites *online* y nuevas vías de participación electrónica. Con la potenciación del uso de la informática y las comunicaciones se persigue fomentar la relación electrónica entre todos los actores con la universidad: personal docente e investigador, personal técnico, de gestión y de administración y servicios, estudiantado y ciudadanía en general.

Las estrategias de ciberseguridad en todos sus niveles, desde la Unión Europea a la última de las entidades, tienen como misión esencial garantizar los derechos de los usuarios mediante la construcción de sistemas de información robustos en un contexto de riesgo. Para ello será necesario establecer una gobernanza adecuada que permita coordinar esfuerzos y garantizar la colaboración en el nivel regional, interuniversitario, nacional y europeo, y con planes de respuesta y contingencia que aseguren su resiliencia ante cualquier tipo de crisis.

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:

1. **Alcance estratégico**: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad en todas las áreas (gestión administrativa y tecnológica, investigación y docencia), de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.
2. **Responsabilidad determinada**: En los sistemas TIC se identificará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios y el responsable de la seguridad de la información, que determina las decisiones para satisfacer los requisitos de seguridad.
3. **Seguridad integral**: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos relacionados con los sistemas TIC, 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 TIC.
4. **Gestión de riesgos**: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Se realizará mediante el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos y la eficacia y el coste de las medidas de seguridad.

   Cuando se traten datos personales la gestión de riesgos deberá tener en cuenta lo dispuesto por el 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 (RGPD) en cuanto a la gestión de riesgos para los derechos y libertades de las personas, riesgos de seguridad y, en su caso, integrará las metodologías de evaluación de impacto relativas a la protección de datos.

5. **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.
6. **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.
7. **Seguridad por defecto**: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

4. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

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

1. **Garantizar la calidad y protección de la información.**
2. **Lograr la plena concienciación de todos los usuarios respecto a la seguridad de la información:** Estos están integrados por el personal docente e investigador, personal técnico, de gestión y de administración y servicios, estudiantado y cualesquiera otros relacionados con los sistemas de información de la universidad.
3. **Gestión de activos de información**: Los activos de información de la universidad se encontrarán inventariados y categorizados y estarán asociados a un responsable.
4. **Seguridad ligada a las personas**: Se implantarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los activos de información reciba la correspondiente información sobre sus responsabilidades y una formación adecuada de modo que se reduzca el riesgo derivado de su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
5. **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.
6. **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 TIC. 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.
7. **Control de acceso**: Se limitará el acceso a los activos de información por parte de usuarios, 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.
8. **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.

9. **Gestión de los incidentes de seguridad**: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad, así como para su notificación a terceros en el marco de procedimientos de colaboración o en cumplimiento de obligaciones legales.
10. **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 acuerdo con las necesidades de nivel de servicio de sus usuarios.
11. **Protección de datos**: En el tratamiento de datos personales, pseudonimizados o anonimizados y en aquellos tratamientos de datos personales orientados a diseñar procesos que repercutan en las personas, se adoptarán las medidas técnicas y organizativas necesarias para diseñar los tratamientos y gestionar los riesgos garantizando el cumplimiento del RGPD y de cualquier otra normativa de desarrollo y el pleno ejercicio de los derechos.
12. **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 Valladolid relacionados con el ejercicio de sus competencias y a todos los usuarios 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 y la normativa de seguridad derivada, siendo responsabilidad del Comité de seguridad de la información disponer los medios necesarios para que la información llegue al personal afectado.

6. MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades de la Universidad de Valladolid y, en particular, la prestación de sus servicios electrónicos está integrado por las siguientes normas:

- Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario.
- Ley 17/2022, de 5 de septiembre, por la que se modifica la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Estatutos de la Universidad de Valladolid, aprobados por Acuerdo 111/2020, de 30 de diciembre, de la Junta de Castilla y León.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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.

- 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.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 3/2015, de 4 de marzo, de Transparencia y Participación Ciudadana de Castilla y León
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- 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.
- Ley 14/2007, de 3 de julio, de Investigación biomédica.
- Ley 3/2003, de 28 de marzo, de Universidades de Castilla y León.

Asimismo, forman parte de este marco normativo el Reglamento por el que se implantan los medios electrónicos que facilitan el acceso de los ciudadanos a los servicios públicos y se crean la sede electrónica y el registro electrónico de la Universidad de Valladolid, aprobado por el Consejo de Gobierno de 11 de junio de 2012, así como las restantes normas aplicables a la administración electrónica de la Universidad de Valladolid, derivadas de las anteriores y publicadas en la sede electrónica, comprendidas dentro del ámbito de aplicación de la presente Política.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1. Criterios utilizados para la organización de la seguridad de la información

La Universidad de Valladolid, teniendo en cuenta lo establecido en el ENS y en la Guía CCN-STIC-801, emprenderá las siguientes acciones para organizar la seguridad de la información:

1. Designará roles de seguridad: responsable de los servicios, responsable de la información, responsable de la seguridad, responsable del sistema y delegado de protección de datos.
2. Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de seguridad de la información. Este órgano se constituirá como un órgano colegiado y se denominará Comité de seguridad de la información.

7.2. Roles y órganos de la seguridad de la información

En la Universidad de Valladolid, en el marco del ENS, los roles y órganos de la seguridad de la información, serán los siguientes:

- **Responsable de los servicios**: gerente.
- **Responsable de la información**: secretario general.
- **Responsable de seguridad de la información**[1]: director técnico en materia de seguridad.

[1] El Responsable de seguridad de la información corresponderá a un cargo o funcionario, de nivel ejecutivo, designado formalmente por el Rector. El Responsable de seguridad de la información no podrá ser un órgano de gobierno unipersonal de la universidad y no deberá tener ninguna responsabilidad sobre la prestación de los servicios TIC, ni deberá estar bajo la dependencia jerárquica del Responsable del Sistema (y viceversa).

- **Responsable del sistema**: director del Servicio de Tecnologías de la Información y Comunicaciones (STIC).
- **Comité de seguridad de la información**:
  - **Presidente**: el responsable de los servicios.
  - **Secretario**: el responsable de la seguridad de la información, que realizará las convocatorias por indicación del presidente, levantará actas de las sesiones y certificará los acuerdos adoptados.
  - **Vocales**:
    - Miembros permanentes:
      - El responsable de la información.
      - El responsable del sistema.
      - La persona titular del vicerrectorado con competencias en materia de tecnología de la información y comunicaciones.
      - La persona del servicio TIC encargada de la gestión económica y presupuestaria.
      - El delegado de protección de datos. Participará con voz, pero sin voto, en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal que impliquen una decisión sobre los fines y los medios del tratamiento, así como siempre que se requiera su participación. En todo caso, si un asunto de esta naturaleza se sometiese a votación, se hará constar siempre en acta la opinión del delegado de protección de datos. Las decisiones del Comité deberán respetar su independencia cuando ejerza la posición y funciones que le otorgan los artículos 38 y 39 RGPD y el Capítulo III y la disposición adicional decimoséptima sobre tratamientos de datos de salud de la LOPDGDD.
    - Miembros no permanentes:
      - El Comité de seguridad de la información podrá convocar a sus reuniones a otros representantes de la universidad o a 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. Los miembros no permanentes presentes en las reuniones del Comité no tendrán derecho a voto.

7.3. Responsabilidades de los roles asociados al Esquema Nacional de Seguridad

7.3.1. Responsables de la información y de los servicios

Serán funciones del responsable de la información y del responsable de los servicios, ejercitable por cualquiera de los dos:

1. Elevar para su aprobación al Comité de seguridad de la información los requisitos de seguridad aplicables a la información (niveles de seguridad de la información) y a los servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD 311/2022,

teniendo en cuenta las propuestas del responsable de seguridad, del responsable del sistema o del delegado de protección de datos.

2. Velar por el buen uso de la información y el buen funcionamiento de los servicios.
3. Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
4. Poner en comunicación del responsable de seguridad cualquier variación respecto a la información y a los servicios de los que es responsable, especialmente la incorporación de nuevos servicios o información a su cargo. El responsable de seguridad dará traslado de dichos cambios al Comité de seguridad de la información en la siguiente reunión.

7.3.2. Responsable de seguridad de la información

Serán funciones del responsable de seguridad de la información:

1. Mantener y verificar el nivel adecuado de seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
2. Promover la formación y concienciación en materia de seguridad de la información.
3. Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, proponer las configuraciones de seguridad necesarias y elaborar documentación del sistema.
4. Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el responsable del sistema o con el Comité de seguridad de la información, en función del asunto.
5. 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.
6. Gestionar las revisiones externas o internas del sistema.
7. Gestionar los procesos de certificación.
8. Elevar al Comité de seguridad de la información la aprobación de cambios y otros requisitos del sistema.
9. Aprobar los procedimientos de seguridad que forman parte del mapa normativo, y no sean competencia del Comité, y poner en su conocimiento las modificaciones que se hayan realizado a lo largo del periodo correspondiente.
10. Coordinar y supervisar los procedimientos de notificación de violación de seguridad junto con el delegado de protección de datos.

7.3.3. Responsable del sistema

Serán funciones del responsable del sistema:

1. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
2. Definir la estructura y la gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.
3. Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

4. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
5. Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el responsable de seguridad y con el Comité de seguridad de la información.
6. Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.

El responsable del sistema podrá atribuir, en su caso, a los responsables de cada área TIC las siguientes funciones de administrador de la seguridad del sistema:

1. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
2. 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.
3. Aprobar los cambios en la configuración vigente del sistema de información.
4. Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
5. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
6. 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.
7. Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
8. Informar al responsable de seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
9. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
10. Cualquier otra función que por su naturaleza pueda atribuirse a otros responsables de área TIC.

7.4. Delegado de protección de datos

Serán funciones del delegado de protección de datos[2]:

1. Informar y asesorar al responsable del tratamiento de datos de la Universidad de Valladolid y a los usuarios que se ocupen del tratamiento de las obligaciones que les incumben en virtud de la normativa vigente en materia de protección de datos.
2. Supervisar el cumplimiento de lo dispuesto en la normativa de seguridad y en las políticas internas de la Universidad de Valladolid en materia de protección de datos, incluida la

[2] Según el art. 36.2 LOPDGDD, cuando el delegado de protección de datos se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

asignación de responsabilidades, la concienciación y formación del personal que participa en las actividades de tratamiento y en las auditorías correspondientes.

3. Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
4. Evaluar el impacto en los derechos y libertades de los interesados ante la ocurrencia de incidentes de seguridad graves que, conforme al RGPD, obliguen a una notificación de violación de seguridad a la autoridad de protección de datos o las personas interesadas, así como coordinar con el soporte del responsable de seguridad el proceso de notificación.
5. Cooperar con la Agencia Española de Protección de Datos cuando esta lo requiera, actuando como punto de contacto para cuestiones relativas a los tratamientos de datos.
6. El delegado de protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
   a) Recabar información sobre las actividades de tratamiento y acceder a los sistemas de información cuando lo requiera, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto.
   b) Supervisar la conformidad de las actividades de tratamiento.
   c) Informar, asesorar y emitir recomendaciones al responsable o al encargado del tratamiento.
   d) Recabar información para supervisar el registro de las actividades de tratamiento.
   e) Supervisar el cumplimiento del principio de la protección de datos desde el diseño y por defecto en el diseño de los sistemas de información.
   f) Emitir informe sobre la necesidad de llevar a cabo evaluaciones de impacto, metodologías, salvaguardas a aplicar, etc.
   g) Asesorar al responsable del tratamiento sobre auditorías, actividades formativas y actividades de tratamiento que requieran especial atención.
   h) Documentar y comunicar inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento las vulneraciones relevantes en materia de protección de datos.
   i) Cuantas funciones le sean atribuidas por la legislación aplicable y su normativa de desarrollo.

7.5. Comité de seguridad de la información

7.5.1. Atribuciones del Comité de seguridad de la información

1. Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que deberá darse cumplida respuesta.
2. 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.
3. Atender las consultas en materia de seguridad de la información de la comunidad universitaria, informando regularmente del estado de la seguridad de la información al equipo de gobierno.

4. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables o entre diferentes unidades administrativas, elevando a los órganos superiores jerárquicamente aquellos casos en los que no tenga suficiente autoridad para decidir.
5. Revisar la Política de seguridad de la información previamente a la aprobación por el Consejo de Gobierno.
6. Aprobar la normativa de uso de medios electrónicos derivada de la presente política de seguridad.
7. Aprobar el conjunto de reglas y procedimientos de seguridad para la implantación del ENS.

7.5.2. Responsabilidades del Comité de seguridad de la información

1. Estar 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.
2. Conocer la relación de entidades de certificación acreditadas y organizaciones, públicas y privadas, certificadas.
3. Estar informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos acuerdos de reconocimiento mutuo de certificados.

7.5.3. Periodicidad de las reuniones y adopción de acuerdos

1. Durante el desarrollo del proyecto de adecuación al ENS, para evaluar el desarrollo del mismo y posibilitar su adecuado seguimiento, el Comité de seguridad de la información se reunirá, al menos, una vez al trimestre.
2. Una vez alcanzada la certificación de conformidad con el ENS de los servicios prestados por la universidad, el Comité de seguridad de la información 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.
3. En cualquier caso, las reuniones se convocarán por el presidente, a través del secretario, a su iniciativa o por mayoría de sus miembros permanentes.
4. Las decisiones se tomarán por mayoría simple de los asistentes a las reuniones, y en caso de empate, se abrirá un nuevo turno de palabra y se procederá a realizar una nueva votación. Si se produce un nuevo empate, decidirá el presidente con su voto de calidad.
5. El Comité podrá establecer sus propias normas de funcionamiento interno y, en lo no previsto, su funcionamiento se regirá supletoriamente por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

7.5.4. Procedimientos de designación

Los miembros del Comité de seguridad de la información serán nombrados en la forma normativamente establecida por la Universidad de Valladolid.

7.6. Oficina de Seguridad de la Información (OSI)

Dentro de la estructura de gobernanza de la ciberseguridad se constituye la Oficina de Seguridad de la Información, cuyas competencias estarán relacionadas con las siguientes áreas de trabajo: adecuación al ENS, normativa y procedimientos de seguridad, gestión de riesgos, análisis y mejora

continua, seguridad en las interconexiones y conectividad, así como otras funciones relacionadas. Estará compuesta por:

- El **director de la OSI** será el responsable de seguridad de la información.
- El **secretario de la OSI**.
- **Todos aquellos especialistas** que el responsable de seguridad en colaboración el responsable del sistema determine que sean necesarios. Entre ellos incluirá un técnico TIC en cada una de las siguientes áreas: redes, sistemas y desarrollo, así como un técnico TIC de centro o departamento de cada uno de los cuatro campus.

Las **funciones de la OSI** serán, entre otras que les puedan ser encomendadas por el Comité de seguridad de la información, las siguientes:

1. Gestión y operativa de la seguridad del proyecto de adecuación, implantación del ENS y gestión de la conformidad con este, análisis y gestión de riesgos y desarrollo y mantenimiento de la normativa en materia de seguridad de la información.
2. Redacción y presentación de propuestas al Comité de seguridad de la información. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al Comité.
3. Promover la mejora continua del sistema de gestión de la seguridad de la información. Para ello se encargará de:
   a) Revisar regularmente esta Política de seguridad de la información para su traslado al Comité de seguridad para su revisión y posterior aprobación.
   b) Elaborar la normativa de seguridad de la información para su aprobación por el Comité de seguridad.
   c) Elaborar y verificar los procedimientos de seguridad de la información y demás documentación para su aprobación por el Comité de seguridad.
   d) Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información.
   e) Elaborar y aprobar los requisitos de formación y cualificación de administradores, técnicos TIC y usuarios desde el punto de vista de seguridad de la información.
   f) 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.
   g) Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones al respecto.
   h) Promover la realización de las auditorías periódicas del ENS que permitan verificar el cumplimiento de las obligaciones de la universidad en materia de seguridad de la información.
4. Vigilancia y detección de amenazas en la operación diaria de los sistemas TIC.

Todas las áreas TIC de la universidad deberán coordinarse con la OSI para la definición y aplicación de las medidas de seguridad en los sistemas e infraestructuras que estén bajo su responsabilidad.

En colaboración con los distintos servicios TIC de la universidad, se llevarán a cabo las siguientes funciones:

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

b) Analizar los eventos de seguridad y registros de actividad de los sistemas.

c) Coordinar las operaciones de seguridad sobre los dispositivos específicos para estas funciones.

d) Responder a incidentes de seguridad realizando un seguimiento de su gestión y recomendando posibles actuaciones al respecto.

e) Atender al Sistema de alerta temprana de incidentes de seguridad (SAT) en las redes corporativas y en las conexiones a Internet de los sistemas.

f) Gestionar vulnerabilidades de aplicaciones y servicios (análisis y determinación de las acciones de subsanación y parcheado).

g) Aplicar técnicas de análisis forense digital y de seguridad.

h) Llevar un servicio de cibervigilancia que posibilite la prospectiva sobre ciberamenazas.

7.6.1. Periodicidad de las reuniones y adopción de acuerdos

1. El director de la OSI coordinará las reuniones de trabajo de sus miembros y trasladará los acuerdos alcanzados al Comité de seguridad de la información, para su aprobación, en su caso.
2. La OSI podrá desarrollar sus funciones en pleno o en grupos de trabajo para el análisis y realización de propuestas específicas. Las propuestas planteadas en la OSI serán sometidas a análisis, debate y aprobación, cuando proceda, por parte del Comité de seguridad de la información.
3. Se reunirá, al menos, una vez cada dos meses y siempre antes de las celebraciones del Comité de seguridad de la información.

7.7. Foro de seguridad TIC de las universidades

El Foro de seguridad TIC se constituye como un punto de encuentro de las universidades en el ámbito del ENS.

La sectorial CRUE-Digitalización, entre cuyas misiones está la de “estudiar las necesidades y aplicaciones de las TIC en la gestión, la docencia y la investigación, proponiendo actuaciones y proyectos conjuntos a las universidades”, dispone de un grupo de trabajo específico de seguridad y auditoría TIC. En dicha sectorial están representadas todas las universidades españolas, tanto públicas como privadas. Dicho grupo de trabajo constituye el marco ideal para ser el foro de seguridad TIC para universidades. Debido al carácter sectorial del mundo universitario, será de gran ayuda en el ámbito de la gobernanza en ciberseguridad.

El funcionamiento del foro se regirá según el Reglamento interno de la sectorial CRUE-Digitalización. En el Foro de seguridad TIC se plantearán, entre otras, las necesidades de seguridad de las universidades adheridas. Las propuestas planteadas por este foro serán trasladadas a cada universidad por sus representantes para su análisis, debate y aprobación, si procede, por parte del Comité de seguridad de la información.

Este Foro de seguridad TIC podrá coordinarse con otros foros de carácter sectorial, local o regional.

8. DATOS PERSONALES

La Universidad de Valladolid tratará los datos personales en el ejercicio de sus funciones según lo dispuesto por el Reglamento (UE) 2016/679, de 27 de abril, General de Protección de Datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y demás normativa que resulte de aplicación y siguiendo las directrices generales de la política de protección de datos que tiene publicada en la página web corporativa.

9. OBLIGACIONES DEL PERSONAL

Todo el personal de la Universidad de Valladolid comprendido dentro del ámbito del ENS atenderá a una o varias sesiones de concienciación en materia de seguridad y protección de datos, al menos una vez al año. Se establecerá un programa para de concienciación continua para 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. En su caso, la formación será obligatoria antes de asumir una función específica, 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 responsable de seguridad será el encargado de realizar el análisis de riesgos, así como de identificar carencias y debilidades para ponerlas en conocimiento del Comité de seguridad de la información.

El Comité de seguridad de la información 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.
- 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 8 de enero, 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.

Los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

11. NOTIFICACIÓN DE INCIDENTES

De conformidad con lo dispuesto en el artículo 33 del RD 311/2022, de 3 de mayo, la Universidad de Valladolid, 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 la citada norma.

Tal y como se establece en el artículo 33 RGPD, en caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la Agencia Española de Protección de Datos, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Deberá determinarse en todo caso, con el soporte del delegado de protección de datos, el alcance del incidente.

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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 de la información su revisión anual y mantenimiento, proponiendo mejoras cuando sea necesario.

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:

a) Primer nivel normativo: constituido por la presente Política de seguridad de la información, la normativa interna del uso de los medios electrónicos y las directrices generales de seguridad aplicables a los organismos o unidades de la universidad a los que sea de aplicación dichos documentos.

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

c) 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.

Cuando resulte procedente, se deberá recabar la opinión de los empleados y empleadas públicos o de sus representantes, sin perjuicio de que se adopten las medidas necesarias para proteger los intereses de la universidad.

Corresponde al Consejo de Gobierno de la Universidad de Valladolid la aprobación de la Política de seguridad de la información de la universidad, siendo el Comité de seguridad de la información el órgano responsable de la aprobación de los restantes documentos, encargándose asimismo de su difusión para que los conozcan las partes interesadas.

Del mismo modo, la presente Política de seguridad de la información complementa a la Política de privacidad de la Universidad de Valladolid, en materia de protección de datos.

La normativa de seguridad, la Política de seguridad de la información y la Normativa interna del uso de los medios electrónicos 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 siguiente URL https://digital.uva.es/unidad/stic/seguridad-de-la-informacion/

13. TERCERAS PARTES

Cuando la Universidad de Valladolid preste servicios a otras organizaciones o maneje su información, se les hará participes 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.

Cuando la Universidad de Valladolid utilice servicios de terceros o les ceda información, se les hará participes de esta Política de seguridad y de la normativa de seguridad que afecte a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en esta 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 estos terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de seguridad.

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 responsable de seguridad que precise los riesgos en que se incurre y la forma de tratarlos, que se remitirá al Comité de seguridad de la información para su evaluación y toma de decisiones.

14. 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 la legislación son un ejemplo de que es necesaria una mejora continua de los sistemas. Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

1. Revisión de la Política de seguridad de la información.
2. Revisión de los servicios e información y su categorización.
3. Ejecución con periodicidad anual del análisis de riesgos.
4. Realización de auditorías internas o, cuando procedan, externas.
5. Revisión de las medidas de seguridad.
6. Revisión y actualización de las normas y procedimientos.

ANEXO I – GLOSARIO DE TËRMINOS

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

Amenaza: Posibilidad de que un activo sea dañado o comprometido por un evento no deseado.

Análisis forense digital: Proceso de investigar y recolectar evidencia digital para resolver delitos informáticos.

Auditoría: Examen sistemático de los procedimientos, prácticas y registros para evaluar la conformidad con los estándares establecidos.

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

Brecha de seguridad: Vulnerabilidad o punto débil en la seguridad que puede ser explotado por amenazas.

Categoría del sistema: Clasificación de un sistema según su nivel de seguridad y protección de datos. El ENS establece tres categorías para los sistemas, básica, media y alta, a fin de seleccionar establecer las medidas de seguridad necesarias de acuerdo con el nivel de riesgo.

CCN: Centro Criptológico Nacional, organismo dependiente del CNI (Centro Nacional de Inteligencia) responsable de la criptología y la seguridad de las comunicaciones.

CCN-CERT: Equipo de Respuesta a Incidentes de Seguridad del Centro Criptológico Nacional.

CERT: Equipo de Respuesta a Incidentes de Seguridad.

Ciberamenaza: Peligro o riesgo para la seguridad de los sistemas y la información en el ámbito digital.

Ciberincidente: Evento no deseado o anomalía que compromete la seguridad de los sistemas o la información en línea.

Ciberseguridad: Conjunto de medidas y prácticas destinadas a proteger los sistemas y la información en el entorno digital.

Cibervigilancia: Monitoreo y supervisión de las actividades en línea para detectar y prevenir amenazas o actividades ilícitas.

Ciclo de vida: Fases o etapas por las que pasa un sistema o un proyecto, desde su concepción hasta su finalización.

Confidencialidad: Propiedad que garantiza que la información solo es accesible a personas autorizadas y no se divulga a terceros no autorizados.

Dato anonimizado: Información que ha sido modificada de tal manera que no se puede asociar con una persona específica.

Dato personal: Información que permite identificar o hacer identificable a una persona física.

Dato pseudonimizado: Información que ha sido modificada de manera que no se puede asociar directamente con una persona, pero se puede volver a identificar utilizando información adicional.

Disponibilidad: Propiedad que garantiza que los sistemas y la información están disponibles y accesibles cuando se necesitan.

ENS: Esquema Nacional de Seguridad. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Evaluación de impacto relativa a la protección de datos: Proceso de identificar y evaluar los riesgos asociados al tratamiento de datos personales.

Gestión del riesgo: Proceso de identificar, evaluar y mitigar los riesgos para garantizar la seguridad de los sistemas y la información.

Gobernanza: Marco de políticas, procesos y responsabilidades para dirigir y controlar una organización en relación con la seguridad y la gestión de riesgos.

Hardware: Componentes físicos de un sistema informático, como computadoras, servidores, dispositivos de red, etc.

Incidente de seguridad: Evento o suceso que compromete la confidencialidad, integridad, autenticidad, trazabilidad o disponibilidad de los sistemas o la información.

Información: Datos procesados y organizados con significado y relevancia.

Integridad: Propiedad que asegura que los datos o la información no han sido alterados de manera no autorizada o involuntaria.

LOPDGDD: Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, normativa española que regula la protección de datos personales. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Medida de seguridad: Acción preventiva o correctiva implementada para proteger los sistemas de información con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Medios electrónicos: Formatos digitales o electrónicos utilizados para almacenar, procesar o transmitir datos e información.

Online: En línea, conectado o disponible a través de internet.

OSI: Oficina de Seguridad de la Información.

Plan de contingencia: Procedimientos y acciones establecidos para hacer frente a eventos no deseados o situaciones de crisis.

Plan de continuidad: Conjunto de medidas y acciones para garantizar la continuidad de las operaciones y servicios en caso de un evento que interrumpa las actividades normales.

Plan de mejora: Estrategia o conjunto de acciones para mejorar la seguridad y la gestión de riesgos en un sistema o una organización.

Política de seguridad de la información: Documento que establece los principios, directrices y responsabilidades para la protección de la información y los sistemas.

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

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

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

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

RGPD: Reglamento General de Protección de Datos, normativa europea que regula la protección de datos personales. 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.

Seguridad de la información: Protección de la confidencialidad, integridad y disponibilidad de la información y los sistemas.

Seguridad física: Medidas y controles implementados para proteger los activos físicos, como edificios, equipos y recursos.

Servicio: Conjunto de actividades o acciones realizadas para satisfacer las necesidades de los usuarios o clientes.

Sistema de alerta temprana de incidentes de seguridad (SAT): Infraestructura y procesos para detectar y responder rápidamente a incidentes de seguridad.

Sistema de información: Conjunto de componentes interrelacionados que recopilan, almacenan, procesan y transmiten información.

Software: Programas de computadora o aplicaciones utilizadas para realizar tareas específicas en un sistema informático.

TIC: Tecnologías de la Información y Comunicación.

Trazabilidad: Capacidad de rastrear y documentar la historia, ubicación y uso de los datos, sistemas o recursos.

Usuario: Persona que utiliza o interactúa con un sistema informático, servicio o aplicación.

Violación de seguridad: Ver brecha de seguridad.

Vulnerabilidad: Debilidad o punto débil en un sistema que puede ser explotado por amenazas para comprometer la seguridad.