I. DISPOSICIONES Y ACUERDOS GENERALES

I.3. Rector

Resolución Rectoral de 7 de febrero 2019 por la que se aprueba el texto revisado de la Política de Seguridad de la Información de la Universidad de Sevilla.

0. Aprobación y entrada en vigor.

Mediante Acuerdo del Consejo de Gobierno de 26 de febrero de 2014, se aprobó la Política de Seguridad de la Información de la Universidad de Sevilla (en adelante US), modificada por la Resolución de 16 de enero de 2017 y publicada en el BOUS de 31 de enero de 2017, dispone, en su apartado 9, que citada Política "será revisada anualmente por la Comisión de Seguridad de la Información y será aprobada por Resolución Rectoral".

La Comisión de Seguridad de la Información en sesión de 27 de noviembre de 2018 acordó proponer al Rector de la US la modificación de la Política vigente desde febrero de 2014 (modificada por la Resolución de 16 de enero de 2017 y publicada en el BOUS de 31 de enero de 2017) para su aprobación por Resolución Rectoral.

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

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

1. Introducción.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (modificado por el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica), establece en su artículo 11 que "todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente."

La consolidación del uso de las nuevas tecnologías en la US exige el establecimiento de un conjunto de actividades y procedimientos para el tratamiento y gestión de los riesgos asociados a la seguridad de la información. La gestión de la seguridad de los sistemas de información es un proceso complejo que incluye a personas, tecnologías, normas y procedimientos.

La aprobación de esta política manifiesta el interés de la US en la gestión de la seguridad de la información. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

La US establecerá las medidas técnicas, organizativas y de control que garanticen la consecución de estos objetivos.

2. Misión de la Universidad de Sevilla.

La US tiene una misión bien definida que se fundamenta en su Estatuto. En el título preliminar, Artículo 1 se encuentran los elementos definitorios de la misión de la Universidad:

La Universidad de Sevilla es una institución de Derecho público, dotada de personalidad jurídica, que desarrolla sus funciones, de acuerdo con la legislación vigente, en régimen de autonomía, y a la que corresponde la prestación del servicio público de educación superior, mediante el estudio, la docencia y la investigación, así como la generación, desarrollo y difusión del conocimiento al servicio de la sociedad y de la ciudadanía.

3. Alcance.

El alcance de la política de seguridad incluye a todos los miembros de la comunidad universitaria y a los organismos o empresas colaboradoras. La política de seguridad es aplicable a todos los sistemas de información de la US y a aquellos que den soporte a sus procesos y afecta a todos los activos de información sustentados en ellos, así como las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos.

En este ámbito no se considera un "recurso TI de la Universidad" aquellos ordenadores personales financiados a título individual, no inventariados a nombre de la US, aunque pudieran ocasionalmente ser usados para labores propias de investigación. Por tanto, quedan fuera de este ámbito dichos elementos, así como las acciones sobre ellos o riesgos de seguridad de tales elementos. No obstante, en el caso de que se acceda a la red corporativa mediante dichos ordenadores personales, quedarán sujetos a las obligaciones establecidas en la presente política de seguridad de la información y normas e instrucciones de desarrollo.

La Política de Seguridad se aplica también a todas aquellas personas, instituciones, entidades o unidades y servicios, sean internos o externos, que hagan uso de los recursos de TI de la US, sea mediante conexión directa o indirecta con los mismos, conexión remota o a través de equipos ajenos a la misma, incluyendo expresamente sus servicios Web. En adelante se considerará a todos ellos "usuarios".

4. Marco normativo.

Esta política se sitúa dentro del marco jurídico definido por las siguientes normas:

De ámbito Europeo:

- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas del mercado interior (Idas) y normas de ejecución.
- 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.
- Directiva (UE) 2016/1148 del Parlamento Europeo y el Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión.
- Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.

De ámbito Estatal:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- 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.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- 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 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y Buen gobierno.
- Ley 39/2105, de 1 de octubre, de Procedimiento Administrativo Común.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Resolución de 7 de octubre de 2016 de la Secretaría de estado de Administraciones Públicas, por el que se aprueba la Instrucción Técnica de Seguridad de Informe de Estado de Seguridad.
- Resolución de 13 de octubre de 2016 de la Secretaría de estado de Administraciones Públicas, por el que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

De ámbito Autonómico:

- Decreto Legislativo 1/2013, de 8 de enero, por el que se aprueba el Texto Refundido de la Ley Andaluza de Universidades.
- Ley 1/2014 de 24 de junio Andaluza de Transparencia Pública de Andalucía.

De ámbito Interno:

- Estatuto de la US.
- Reglamento de creación y regulación de la Sede Electrónica de la US (Acuerdo 11.6/CG 27-6-12).
- Resolución de la Secretaria General de la US, de 20 de marzo de 2013, por la que se crea el Sello Electrónico para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada.
- Resolución de la Secretaria General de la US, de 20 de marzo de 2013, por la que se modifica la relación de procedimientos y servicios susceptibles de presentación en el registro electrónico.

Otras normas que en la actualidad o en el futuro, de carácter general o interno, resulten de aplicación a la US en el marco de esta Política de Seguridad.

5. Organización de la seguridad.

Para garantizar que todas las etapas del ciclo de vida de protección de la información sean realizadas de manera apropiada y las responsabilidades para su ejecución sean asignadas adecuadamente, la US establece una estructura que permite promover la aplicación consistente de la presente política y acomodar efectivamente los frecuentes cambios tecnológicos y organizacionales.

Para ello, se definen los siguientes Comités y Roles generales relacionados con su participación en la gestión y supervisión de la seguridad de la información:

- Comisión de Seguridad de la Información.
- Responsable de la Información.
- Responsable del Servicio.
- Responsable de la Seguridad de la Información.
- Responsable los Sistemas de Información.

6. Comisión de Seguridad de la Información.

La Comisión de Seguridad de la Información es el órgano de gestión interna al que compete la Seguridad de la Información en la US.

Esta Comisión estará compuesta por:

- El máximo responsable con competencias en materia de TI, como presidente de la misma.
- El máximo responsable de los Recursos Humanos.
- El Responsable de la Información.
- El Responsable del Servicio.
- El máximo responsable de los Servicios Jurídicos de la US.
- El Responsable de la Seguridad de la Información (que actuará como Secretario).
- El Delegado de Protección de Datos de la US.
- El Responsable del Sistema.

La Comisión de Seguridad de la Información recabará información y auxilio de todas las áreas de la US cuando así lo considere necesario. Todas las áreas, servicios y unidades de la US están obligadas a informar y prestar apoyo a la Comisión de Seguridad cuando ésta lo requiera.

La Comisión de Seguridad de la Información tiene las siguientes funciones y responsabilidades:

- Elaborar la estrategia de evolución de la US en lo que respecta a la seguridad de la información. Identificar, revisar y proponer objetivos estratégicos en materia de seguridad de la información.
- Informar del estado de la seguridad de la información a los Órganos de Gobierno de la US.
- Proponer al Consejo de Gobierno la aprobación de la política de seguridad de la información.
- Proponer al Rector la aprobación de las modificaciones sobre la política de seguridad.
- Proponer al Rector la aprobación de las normativas y reglamentos de seguridad relacionados con la aplicación del ENS.
- Proponer las iniciativas principales para mejorar la gestión de la seguridad de la información, incluyendo la divulgación de la política y normativas de seguridad.

- Coordinar la adopción de acciones y medidas encaminadas a la adaptación de la US al Esquema Nacional de Seguridad.
- Asegurar la disponibilidad de los recursos necesarios para llevar a cabo los planes de acción relacionados con la seguridad de la información o priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Proponer la designación de los responsables encargados de la aplicación y supervisión de las medidas de seguridad.
- Aprobación de los procedimientos de seguridad de la US cuando así lo solicite el Responsable de Seguridad.
- Realizar una revisión periódica del contenido de la Política de Seguridad y una propuesta de actualización cuando sea necesario.
- Resolver los conflictos entre los diferentes responsables.
- Supervisión y aprobación de las tareas de seguimiento del Esquema Nacional de Seguridad:
    - º Grado de cumplimiento del plan de adecuación.
    - º Revisión de los resultados obtenidos en las diferentes actualizaciones del análisis de riesgos y los niveles de riesgo alcanzados.
    - º Resultados de las auditorías bienales que se realicen y otros informes asociados a la idoneidad de los controles de seguridad implantados, identificando las causas origen de las excepciones que pudieran existir y proponiendo acciones de mejora.

6.1. Responsable de la Información.

La figura del responsable de la Información recaerá en el Secretario General de la US. Tiene las siguientes funciones y responsabilidades:

Establecer los requisitos de seguridad que deban ser garantizados en el tratamiento de la información de la que es responsable.

Valorar para cada información contemplada en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).

Trabajar en colaboración con el Responsable de Seguridad de la Información y el de los Sistemas de Información en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

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

6.2. Responsable del Servicio.

La figura del Responsable del Servicio recaerá en el Gerente de la US. Tiene las siguientes funciones y responsabilidades:

- Establecer los requisitos de los servicios en materia de seguridad que deban ser garantizados en el tratamiento de la información.
- Valorar para cada servicio contemplado en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).
- Trabajar en colaboración con el Responsable de Seguridad de la información en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

6.3. Responsable de la Seguridad de la Información.

El Responsable de Seguridad de la Información será el cargo competente en materia de Seguridad de la Información en el ámbito del ENS y tiene las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TI en el ámbito de cumplimiento del ENS.
- Instar y asesorar en la valoración de los requisitos de seguridad que deban ser garantizados en el tratamiento de la información por parte de los nuevos servicios electrónicos prestados por la US según el criterio de valoración establecido por el artículo 43 del ENS.
- Realizar o instar la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la US en materia de seguridad.
- Supervisar el estado de seguridad del sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar un informe periódico de seguridad, que incluya los incidentes más relevantes del periodo.
- Elaborar la normativa de seguridad.
- Promover la formación y concienciación en materia de seguridad de la información del personal de la US y en especial, del personal del Servicio Informático involucrado en las labores de gestión de los sistemas de información que dan soporte a los procesos de Administración Electrónica de la US.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Aprobar los procedimientos de seguridad elaborados por el Responsable del Sistema cuando en virtud del contenido definido no requieran la revisión y aprobación de la Comisión de Seguridad.
- Elaborar como secretario de la Comisión los siguientes informes periódicos:
    - º Resumen consolidado de las actuaciones llevadas a cabo y en curso dentro del desarrollo del Plan de adecuación del ENS aprobado.
    - º Resumen consolidado de los incidentes de seguridad registrados desde la última reunión de la Comisión.
    - º Valoración del estado de la seguridad de los sistemas de información afectados por el ENS y la evolución de los niveles de riesgo a los que están expuestos.
    - º Resumen consolidado de los procedimientos de seguridad aprobados por el Responsable de Seguridad desde la última reunión de la Comisión.

El Responsable de la Seguridad de la Información actuará como el secretario de la Comisión de Seguridad de la Información y como tal:

- Convoca las reuniones de la Comisión de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones de la Comisión, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones de la Comisión de Seguridad.

6.4. Delegado de Protección de Datos.

El Delegado de Protección de Datos es nombrado por el Rector. Tiene las siguientes responsabilidades dentro del ámbito de la protección de datos personales:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y demás normativas en materia de protección de datos personales.
- Supervisar el cumplimiento de lo dispuesto en el RGPD y demás normativas en materia de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales.
- Supervisar la asignación de responsabilidades.
- Supervisar la concienciación y formación del personal que participa en las operaciones de tratamiento.
- Supervisar las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos.
- Supervisar su aplicación de conformidad con el artículo 35 del RGPD.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36.
- Realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

6.5. Responsable del Sistema.

El Responsable del Sistema será el cargo que ostente la máxima autoridad del Sistema de Información de la US. Tendrán las siguientes responsabilidades dentro de su ámbito de competencias:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, incluyendo las especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la tipología y los procedimientos de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Establecer planes de contingencia y los procesos de análisis y gestión de riesgos en el Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar la documentación de seguridad del Sistema.

- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, efectuar la comunicación al Responsable de Seguridad de la información o a quién éste determine.

6.6. Procedimiento de designación.

El desempeño de cualquiera de las responsabilidades definidas en esta política de seguridad y en el ENS vendrá determinado por el acceso a los diferentes cargos o destinos, estatutarios o no, que han quedado vinculadas a ellas.

En el caso de que desapareciese o cambiara de denominación de alguno de los puestos vinculados a la aplicación del ENS, será competencia del Rector asignar el nuevo puesto al que quedará vinculada la figura.

7. Obligaciones del personal.

Todos los miembros de la US 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 de la Comisión de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todo el personal de la US debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como que ellos mismos son una pieza esencial para el mantenimiento y mejora de la seguridad.

Se establecerá un programa de concienciación continua para atender a todos los miembros de la US, en particular a los de nueva incorporación. Las personas con responsabilidad en el uso, operación o administración de sistemas TI recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

8. Desarrollo de la Política de Seguridad de la Información.

El marco normativo en materia de seguridad establecido por la US está estructurado en diferentes niveles de forma que los objetivos planteados por el presente documento tengan un desarrollo reglamentario que permita definir y concretar regulaciones y restricciones que sean aplicables sobre los sistemas de información o aplicables al personal que gestiona o utiliza dichos sistemas.

La US estructura su marco normativo en los siguientes tipos de documentos:

- La presente Política de Seguridad de la Información que establece los requisitos y criterios de protección en el ámbito de la US y servirá de guía para la creación de normas de seguridad.
- Las normas de seguridad que definen qué hay que proteger y los requisitos de seguridad deseados. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política. La US diferencia entre Normativa general, aplicable a todo el ámbito universitario y Normativa técnica aplicable sobre el área de gestión y operación de las tecnologías de la información. Los procedimientos de seguridad en los que se describe de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Son documentos que especifican cómo llevar a cabo

las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

Además, pueden considerarse dos tipos más de documentos:

- Basándose en los procedimientos de seguridad, y para entornos o sistemas de información concretos, podrán elaborarse instrucciones técnicas de seguridad que documenten de forma explícita y detallada las acciones técnicas a realizar en la ejecución del procedimiento o las tareas a considerar cuando se ejecute un procedimiento.
- También podrán existir, como desarrollo de la propia política de seguridad o de cualquiera de las normas existentes, las normas de uso que establecen las normas de comportamiento que deben cumplir los usuarios en el uso de los sistemas de información. Estos documentos destinados a usuario final resumirán y trasladarán los requisitos de seguridad a contemplar en la utilización o uso de determinadas tecnologías o servicios de manera concisa y fácilmente comprensible, así como lo que se considerará uso indebido y la responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

La US dispone de un documento de seguridad que recoge los ficheros y tratamientos de datos afectados y los responsables correspondientes según lo establecido en 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) y el correspondiente Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD). Todos los sistemas de información de la US se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad y cumplirán a su vez la presente política cuando los ficheros de datos de carácter personal se encuentren dentro del ámbito de aplicación de las leyes 39/2015 y 40/2015.

9. Gestión de riesgos.

Las decisiones en materia de seguridad deben basarse en el análisis y gestión de riesgos como proceso esencial de seguridad, que deberá mantenerse permanentemente actualizado. La evaluación de riesgos identifica las amenazas y vulnerabilidades y debe ser suficientemente amplia para abarcar los principales factores internos y externos tales como factores tecnológicos, físicos y humanos, políticos y servicios de terceros con implicaciones 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, los riesgos a los que estén expuestos y las medidas de seguridad. Debido a la creciente interconexión de los sistemas de información, la evaluación de riesgos debe incluir la consideración de los posibles daños que pueden proceder de otros o ser causados por terceras personas.

Todos los sistemas sujetos a esta Política deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez cada año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.

- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

10. Proceso de revisión de la política de seguridad.

El marco normativo en materia de seguridad de la US se revisará de la siguiente forma:

- La presente Política de Seguridad de la Información será revisada regularmente, y de forma excepcional siempre que haya cambios sustanciales en la Organización, por la Comisión de Seguridad de la Información y será aprobada por Resolución Rectoral.
- Las normas de seguridad serán aprobadas por Resolución Rectoral a propuesta de la Comisión de Seguridad de la Información.
- Los procedimientos de seguridad serán aprobados por la Comisión de Seguridad de la Información cuando así lo solicite el Responsable de Seguridad.

Toda nueva versión de un documento aprobado dentro del marco normativo será comunicada según el alcance de uso del documento y el nivel de difusión requerido de forma que el personal pueda eliminar las versiones de los documentos obsoletos.

11. Terceras partes.

Cuando la US preste servicios a otros organismos o maneje información de los mismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales de comunicación y colaboración entre los respectivos órganos de coordinación de la seguridad de la información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

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

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

El Rector,
Miguel Ángel Castro Arroyo.

APÉNDICE I:

LENGUAJE DE GÉNERO

Las referencias a personas o colectivos figuran en la presente política en género masculino como género gramatical no marcado. Cuando proceda, será válida la cita de los preceptos correspondientes en género femenino.

APÉNDICE II:

GLOSARIO

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

Datos de carácter personal. Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

ENS. Esquema Nacional de Seguridad. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado por el RD 951/2015 de 23 de Octubre.

Gestión de incidentes. Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

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

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

Información. Caso concreto de un cierto tipo de información.

LOPD. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (cualquier información concerniente a personas físicas identificadas o identificables).

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

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

Responsable de la información. Rol que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

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

Responsable del servicio. Rol que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema. Persona que se encarga de la explotación del sistema de información.

RGPD. 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.

Servicio. Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

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