UNIVERSIDAD DE
MURCIA

Candidatura premios MetaRed 2022

Estrategia de ciberseguridad

de la Universidad de Murcia

Murcia, 17 de junio de 2022

Avda. Teniente Flomesta, 5. Edif. Convalecencia. 30003 Murcia
T. 868 88 3000 – **www.um.es**

Resumen

La Universidad de Murcia consciente de la importancia de la ciberseguridad y de la necesidad de incrementar su nivel de madurez estableció, en el año 2019, una ambiciosa **estrategia de mejora de la seguridad** de la organización en distintos ámbitos de actuación.

En primer lugar, se establecieron las acciones necesarias para el **gobierno de la ciberseguridad** por parte de la dirección de la institución y los responsables de la información, los servicios y la seguridad. Fruto de esta implicación global, se creó la **Comisión de Seguridad** como un órgano global que analizara y estableciera el rumbo de la estrategia de ciberseguridad corporativa.

Posteriormente, se realizó un importante trabajo de categorización de sistemas corporativos, análisis de riesgos, declaración de aplicabilidad, implantación de un SGSI, etc., con el objetivo de cumplir el **Esquema Nacional de Seguridad (ENS)**, de obligado cumplimiento para las Administraciones Públicas Españolas. Objetivo que fue cumplido en diciembre de 2019, situando a la **Universidad de Murcia como cuarta universidad pública española en conseguir este distintivo y segunda universidad en conseguir su recertificación en enero de 2022**.

Este hito nos ha permitido apoyar a otras universidades y administraciones en materia de ciberseguridad. En concreto, fruto de la colaboración con CRUE-TIC, sectorial TIC de la CRUE Universidades Españolas, y el Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI), hemos trabajo en la **creación de una guía de *"perfil de cumplimiento del ENS" [CCN-STIC 881]* para el sector de las Educación Superior en España**.

Adicionalmente, la Universidad de Murcia ha estado trabajando en la creación de una fuerza de detección, prevención y reacción capaz de velar por la seguridad de la organización y toda su comunidad universitaria. Fruto de esto, en 2021 se creó el **Security Operations Center (SOC) de la Universidad de Murcia** donde se establecieron procedimientos normalizados de respuesta, se formó un equipo técnico de trabajo y se le dotó de las tecnologías necesarias para la detección temprana, pentesting y monitorización continúa de sistemas, personas y comportamientos dentro de la institución.

Por último, durante todo este tiempo se ha evolucionado en la creación de un amplio **plan de formación y concienciación en materia de ciberseguridad** que fomente una cultura basada en el conocimiento de los riesgos que las nuevas tecnologías pueden ocasionar en el trabajo diario de nuestros usuarios. Un plan de formación anual que cada año tiene un impacto directo en 35.000 usuarios y con el que estamos contribuyendo a crear una universidad más segura.

Contexto

En los últimos años el sector de la educación superior ha sido uno de los sectores con mayor incremento del número de ciberataques. Actualmente ocupa la tercera posición a nivel mundial, tan solo superado por el sector bancario y sanitario.

El robo de información de gran valor de investigaciones, patentes y material de conocimiento, la extorsión económica y la desestabilización de los países son los principales objetivos de estos ciberatacantes.

Todas las Instituciones de Educación Superior, tanto públicas, como privadas, han tenido que afrontar un importante reto para incrementar su madurez de Seguridad de la Información en general y ciberseguridad o Seguridad Informática en particular.

En las Universidades públicas estas acciones han presentado y está presentado un **doble desafío**.

1. Por un lado, es necesario un **cambio cultural** en la organización a distintos niveles:

    a. Dirección: deben ser conscientes del riesgo al que está expuesta la universidad y tomar decisiones sobre tomar acciones para minimizar su impacto o asumirlo. En este sentido, las inversiones en ciberseguridad tendrán un incremento considerable en materia de infraestructura y recursos humanos.

    b. Comunidad universitaria: estudiantes, personal docente e investigador, personal de administración y servicios y otros colectivos deben de ser conscientes de la importancia y valor que tiene la información que manejan y cómo protegerla.

    c. Área IT: como equipo fuertemente vinculado con la ciberseguridad será necesario un esfuerzo en integración y compartición de información para obtener una visión holística de posibles vulnerabilidades y mejoras en prevención y recuperación.

2. Por otro lado, debemos contar con **tecnologías, procesos y personas** capaces de velar por prevención, detección y reacción de la universidad.

2. Desarrollo del proyecto

La Universidad de Murcia, consciente de estos importantes retos, comenzó un ambicioso proyecto de ciberseguridad global para presentar respuesta a estos dos desafíos.

2.1. Actividades en materia de GRC (Gobierno, Riesgo y Cumplimiento)

Para ello, dentro del **Plan de Transformación Digital**, que la institución realizó en 2020, se establecía como objetivo prioritario el ***"refuerzo de la capacidad de la Universidad de Murcia en materia de ciberseguridad"***.

OP 7.3. Reforzar la capacidad de la Universidad de Murcia en materia de ciberseguridad

1. Diseñar y ejecutar acciones de formación y concienciación en ciberseguridad aplicada a los diferentes perfiles que componen la comunidad universitaria, con el fin de hacerlos conocedores de los puntos de ataque y de las recomendaciones a seguir.

2. Velar de forma preventiva por la seguridad de la universidad y sus usuarios mediante equipos humanos y técnicos de vigilancia continua ante posibles amenazas y vulnerabilidades.

3. Establecer mecanismos de resiliencia y de recuperación ante posibles ciberincidencias que permitan analizar los sistemas o usuarios afectados, su corrección y vuelta a la normalidad en el menor tiempo posible y con el mínimo impacto en la universidad.

4. Revisión de controles de seguridad (auditoría) y mejora de procesos internos para el aseguramiento de la normativa de obligado cumplimiento en materia de seguridad de la información en las Administraciones Públicas (Esquema Nacional de Seguridad – ENS).

Así mismo, el Plan Estratégico de IT cuenta con una línea exclusiva dedicada a la gestión de la seguridad informática y 4 objetivos concretos.

Línea 5

Gestión de la Seguridad

OB 5.1.	Garantizar la seguridad de nuestros usuarios, sistemas y de la información
OB 5.2.	Aplicar buenas prácticas en la gestión la seguridad
OB 5.3.	Garantizar la autorización y el control de acceso
OB 5.4.	Concienciar a la comunidad universitaria de la importancia de la ciberseguridad

OB 5.1. **Garantizar la seguridad de nuestros usuarios, sistemas y de la información**

- Potenciar el Centro de Operaciones de Ciberseguridad, SOC, para mejorar la seguridad integral.
- Reforzar los sistemas de seguridad perimetral y transversal de detección de intrusiones.
- Garantizar la adecuada actualización y cambio en los sistemas.
- Reforzar los sistemas de seguridad de los endpoints (equipos de usuario, correo electrónico, etc).

OB 5.2. **Aplicar buenas prácticas en la gestión la seguridad**

- Renovar la certificación del Esquema Nacional de Seguridad, ENS.
- Incorporar a la metodología de desarrollo los procesos de seguridad y privacidad que permitan garantizar esta desde las etapas iniciales de diseño.
- Realizar de forma periódica auditorías internas para analizar el nivel de seguridad.
- Planificar y llevar a cabo pruebas de recuperación de los sistemas.

OB 5.3. **Garantizar la autorización y el control de acceso**

- Desarrollar y aprobar la normativa relativa a los derechos de acceso a aplicaciones y servicios TI de los diferentes colectivos de la universidad.
- Implantar una herramienta para la gestión de autorizaciones por parte de la Secretaria General, accesible para los responsables de los diferentes sistemas de información y que permita a cada usuario consultar los servicios TI que tiene autorizados.
- Poner en marcha un auto registro fehaciente de usuarios externos que permita ofrecer a éstos servicios personalizados de forma segura a través del Portal de Servicios.

OB 5.4. **Concienciar a la comunidad universitaria de la importancia de la ciberseguridad**

- Poner en marcha acciones de formación sobre ciberseguridad dirigidas tanto a personal como a estudiantes.
- Ampliar la información sobre recomendaciones de ciberseguridad con contenido más cercanos al usuario (FAQs, videotutoriales, TIPs, etc.).
- Definir los protocolos de aviso e información a los posibles afectados ante incidencias de seguridad.
- Organizar campañas de sensibilización de la importancia de la ciberseguridad.

Estas acciones ponen de manifiesto la importancia que a nivel estratégico tiene la ciberseguridad para la Universidad de Murcia, contando con un respaldo absoluto por parte de la dirección, algo totalmente necesario para acometer un plan de ciberseguridad de garantías y futuro, como primer paso al desarrollo del resto de acciones.

2.2. Actividades en materia de cumplimiento normativo

Tras alinear la ciberseguridad con la estrategia de negocio de la universidad, el siguiente paso necesario era el cumplimiento normativo. En concreto, la Universidad de Murcia consiguió la certificación en el Esquema Nacional de Seguridad (ENS) en el año 2019, convirtiéndose en **la cuarta universidad española en conseguir esta certificación y la que mayor número de subsistemas certificó.**

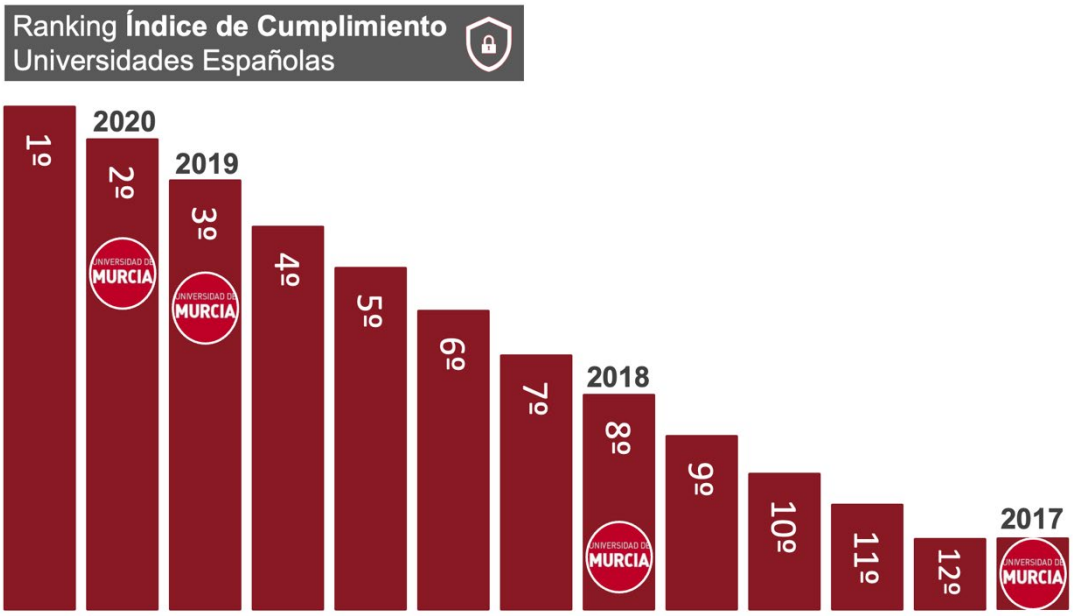
Así mismo, en el año 2022 la Universidad de Murcia se convirtió en la **segunda universidad en conseguir la recertificación**, ampliando el ámbito de su alcance.

Este esfuerzo en el cumplimiento normativo ha permitido un incremento sustancial en el nivel de madurez de ciberseguridad de la institución. Así como posicionarla como un referente nacional e internacional en el sector. En concreto, a nivel nacional esta experiencia le ha permitido participar en la creación del nuevo perfil de cumplimiento del ENS para universidades de la guía CCN-STIC 881 del Centro Nacional de Criptología (CCN) dependiente del CNI, en colaboración con CRUE TIC, y a nivel internacional, ser coordinadora del Grupo de Trabajo Internacional de Ciberseguridad de la Red Iberoamericana de CIO de universidades.

Los principales indicadores a nivel de cumplimiento y madurez reflejados en el informe INES del CCN-CERT son los siguientes:

Índice de cumplimiento

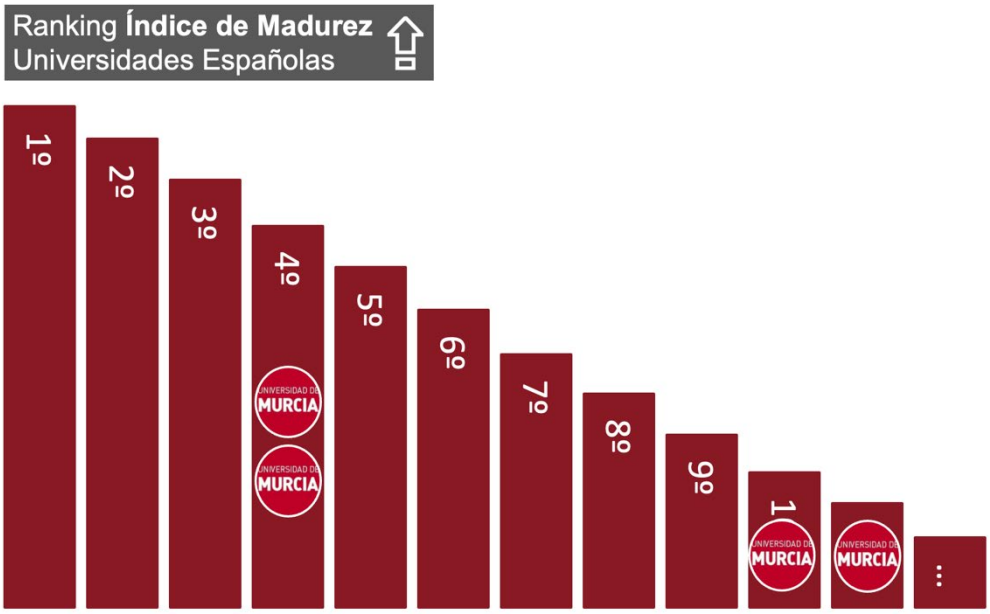
	UM	Media ES	UM	Media ES	UM	Media ES	UM	Media ES
	2020	**2020**	**2019**	**2019**	**2018**	**2018**	**2017**	**2017**
Categoría Básica	100	86,36	100	85,6	No aplica	83,33	76,79	73,8
Categoría Media	98,81	67,04	97,62	65,48	81,33	64,26	76,79	60,7

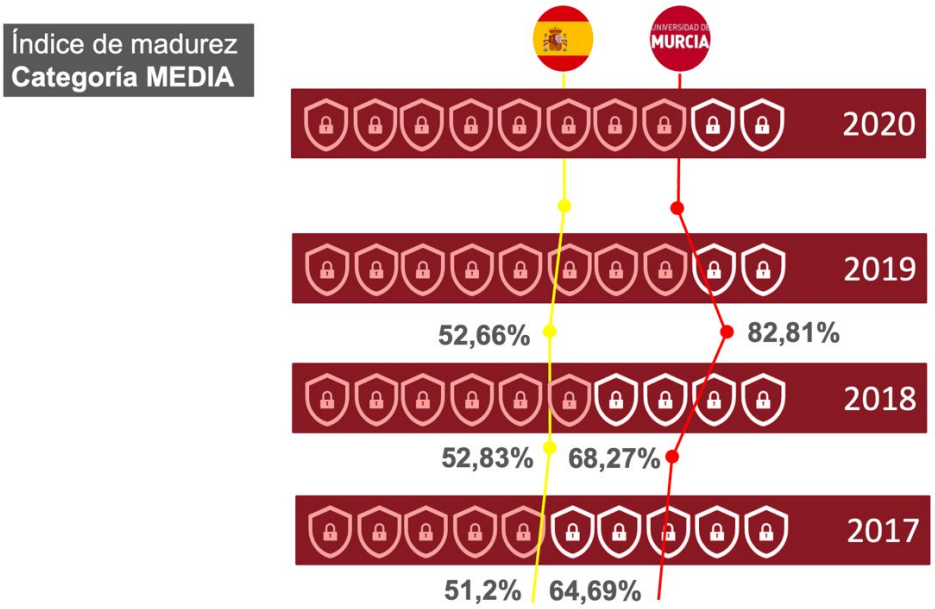


Índice de madurez

	UM 2020	Media ES 2020	UM 2019	Media ES 2019	UM 2018	Media ES 2018	UM 2017	Media ES 2017
Categoría Básica	79,65	54,75	83,28	52,27	No aplica	52,27	64,69	48,8
Categoría Media	79,84	54,05	82,81	52,66	68,27	51,83	64,69	51,2

	2020	2019	2018	2017
Índice de Madurez – Ranking (categoría MEDIA)	4	4	10	11
Índice de Cumplimiento – Ranking (categoría MEDIA)	4	4	10	11


Ranking Índice de Madurez
Universidades Españolas
1º
2º
3º
4º
5º
6º
7º
8º
9º
1
...


Índice de madurez
Categoría MEDIA
2020
2019
52,66%
82,81%
2018
52,83%
68,27%
2017
51,2%
64,69%

Marcos de control ENS

	UM 2020	Media ES 2020	UM 2019	Media ES 2019	UM 2018	Media ES 2018	UM 2017	Media ES 2017
Marco organizativo	82,50%	56,25%	75,00%	55,00%	64,75%	50,00%	65,00%	52,00%
Marco operacional	82,22%	51,48%	82,17%	53,27%	68,52%	51,45%	63,00%	51,50%
Medidas de protección	85,16%	54,32%	85,16%	54,32%	68,48%	52,15%	68,00%	50,30%
Procesos críticos	73,75	53,47	83,13	51,08	64,13	46,69	65,6	49,1

Lo que muestra un incremento notable en el nivel de madurez en los diferentes marcos establecidos por el ENS desde el año 2017 hasta 2020. Valores incrementados tras la actual renovación del sello ENS en el primer trimestre de 2022.

2.3. Actividades técnicas/operativas

Por otro lado, como acciones complementarias y necesarias al *compliance* regulado por el ENS y otras normativas se hace necesario contar con una parte ejecutiva que vele por la protección de la institución.

Para este fin, en el año 2020 la Universidad de Murcia comenzó un **proyecto para la creación de Un Security Operation Center (SOC)** que actuara como "brazo armado" de la ciberseguridad de la organización.

Este SOC es el punto de unión para la integración de:

1. **Tecnologías** que nos permitan reacción de forma preventiva y reactiva ante posibles ciberataques. Por ejemplo, implantación de un SIEM, soluciones de protección de endpoints (EDR), firewall este-oeste, herramientas de ciberinteligencia, pentesting, desarrollo seguro, etc.

2. **Procesos** y procedimiento que establezcan, de forma clara y concisa, las acciones necesarias para la correcta ejecución de diversas tareas cotidianas en el área IT y ciberseguridad: puesta en marcha de aplicaciones, gestión del cambio, gestión de ciberincidentes, respuesta a ransomware, etc.

3. **Personas**: el activo más importante, capaz de sacar el máximo valor a las tecnologías y procesos disponibles para maximizar la protección de toda la comunidad universitaria.

El equipo técnico de detección de ciberataques detecto, a modo de ejemplo, los siguientes eventos en las diferentes herramientas de detección y prevención:

Categoría	**Abril**	**Marzo**
Conexión con Botnet Potencial	920.845	352.015
Exploit	13.805	6.452
Inicios fallidos de sesión	2.730	509
Alteraciones del sistema	1.734	245
Ejecución remota de código	415	201
SQL Injection	144	112
Violación de políticas	122	50
DOS	88	44
Actividad sospechosa	48	29
Buffer Overflow	43	12
Malware	14	2
Troyanos	6	2
Ejecución de comando	3	1
Exploit web	1	1

Estas cifras ponen de manifiesto la importancia de contar con un equipo preventivo que minimice la exposición de la infraestructura y personas de nuestra universidad, reduciendo los posibles vectores de ataque y la superficie expuesta de la institución.

A pesar de los esfuerzos, está claro que no existe una seguridad total, derivando en ciberincidentes de impacto crítico, muy alto o alto los siguientes:

Incidentes	**2020**	**2019**
Total impacto crítico, muy alto o alto	2	2
Días resolución 50% de los incidentes de impacto crítico, muy alto o alto	57	24
Días resolución 90% de los incidentes de impacto crítico, muy alto o alto	57	24
Número incidentes de impacto crítico, muy alto o alto que llevan abiertas más de 21 días	2	0

3. Equipo de desarrollo y proveedores

Al igual que la ciberseguridad es un área trasversal que afecta a todas las secciones de la universidad, el equipo necesario para el correcto desarrollo de las acciones de seguridad abarca desde el diseño de la estrategia de negocio, alineación del área IT, concienciación y formación a la comunidad universitaria y el equipo de prevención y respuesta a incidentes.

En la Universidad de Murcia los principales actores involucrados son los siguientes:

1	Equipo rectoral	Liderazgo ante el cambio cultura. Involucración de toda la comunidad universitaria.
2	Vicerrector de Estrategia y Universidad Digital	Alineación de los objetivos de ciberseguridad con los objetivos de negocio. Inversiones.
3	Responsable de Seguridad	Gobierno, riesgo y cumplimiento.
4	Área IT y Comité Técnico de Seguridad	Operación, bastionado y recuperación.
5	Security Operations Center (SOC)	Prevención, detección, identificación, respuesta y recuperación ante ciberincidentes. Concienciación y formación.
6	Comunidad universitaria	Concienciación y formación.

4. Conclusiones

Con estas acciones la Universidad de Murcia incrementa su nivel de madurez en ciberseguridad con el objetivo de reducir el riesgo y exposición a futuros ciberataques y ciberamenazas. Se trata de una estrategia global que integra: Personas, Tecnologías y Procesos y basada en tres marcos de actuación:

- Gobierno, riesgo y cumplimiento.
- Cumplimiento normativo.
- Operación.

Las acciones acometidas para la mejora de la ciberseguridad de la Universidad de Murcia tienen una repercusión directa en toda la comunidad universitaria de la nuestra universidad, un total de 38.876 personas.

Así mismo, lo dispuesto en el ENS permite satisfacer los principios de actuación y los requisitos de seguridad de las Administraciones Públicas que les permitan alcanzar sus objetivos. Para los ciudadanos, destinatarios últimos del servicio público, supone la garantía de que las entidades públicas con las que se relacionan reúnen las condiciones de seguridad necesarias para salvaguardar su información y sus derechos.

Por último, aplicaría un impacto directo en otros organismos, instituciones y empresas con las que la Universidad de Murcia establece relaciones durante el ejercicio de sus distintas actividades. Por ejemplo, transferencia tecnológica, investigación conjunta, servicios públicos, etc.

4.1. Próximos pasos

Según la normativa vigente en materia de ENS debe ser renovada su certificación cada dos años por una empresa auditora habilitada por el CCN. Durante el primer trimestre de 2022 hemos abordado una primera renovación incrementando el número de subsistemas certificados e incrementando el nivel de madurez del resto, siguiendo las observaciones y mejoras propuestas por la auditoria inicial. La siguiente recertificación será en 2024.

Así mismo, durante los próximos años será necesario mejorar los servicios del Security Operations Center (SOC) corporativo en lo relativo a personas, procedimientos y herramientas para la detección preventiva de vulnerabilidades y posibles amenazas.

Por otro lado, la labor de concienciación seguirá siendo un factor clave en la ciberseguridad de la Universidad de Murcia. Para ello, se continuará trabajando en el plan de formación y concienciación en ciberseguridad anual.