Marco Legal

USTIC-Unidad de Seguridad TIC

Marco legal aplicable

En esta página se incluyen las leyes y normas de aplicación, tanto a la Seguridad de la Información como a la Protección de Datos Personales, agrupadas en cuatro apartados, así como las principales Guías y Buenas Prácticas en ambas materias.

[USTIC-Unidad de Seguridad TIC] [Regulación Corporativa] [Regulación Autonómica] [Regulación Nacional] [Regulación Europea] [Instrucciones Técnicas de Seguridad (ITS)] [Guías CCN-CERT] [Buenas Prácticas CCN-CERT]

Leyes y normas de aplicación

Regulación Corporativa

Resolución de 8 de abril de 2021, de la Dirección Gerencia del Servicio Andaluz de Salud, por la que se aprueba la **Política de Seguridad de las Tecnologías de la información y la comunicación del Servicio Andaluz de Salud.**	Resolucion 8 de abril Politica Seguridad TIC SAS.pdf
Resolución de 26 de marzo de 2021, de la Dirección Gerencia del Servicio Andaluz de Salud, por la que se crea el **Comité de Seguridad Interior y Seguridad de las Tecnologías de la Información y Comunicaciones del Servicio Andaluz de Salud** y se determinan su composición, funciones y bases de su funcionamiento	Resolucion 26_03_2021 Creacion CSISTIC SAS.pdf
Resolución de 29 de junio de 2023, de la Dirección Gerencia del Servicio Andaluz de Salud, por la que se dictan **I nstrucciones sobre la tramitación de convenios administrativos y protocolos generales de actuación en el ámbito del Servicio Andaluz de Salud**.	Resol_0062_23_Modelos_Normalizados_de Convenios.pdf

Regulación Autonómica

Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el **Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía.**	CodigoDeConductaUsoTIC_JA_BOJA20-208-00009.pdf
Decreto 1/2011, de 11 de enero, por el que se establece la Política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.	Decreto1_2011 Politica Seg JdA.pdf
Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la Política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.	Decreto 70-2017 Politica Seg JdA.pdf
Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.	Orden 9-2016 Desarrollo Politica Seg. JdA..pdf
Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC.	Resolucion 13-07-2018 Gestion Incidentes seguridad TIC.pdf
Resolución de 26 de enero de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre integración en el Centro de Seguridad TIC Andalucía-CERT.	Resolucion 26-01-2018 Andalucia CERT.pdf
Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.	Decreto 622-2019 de administración electrónica Junta de Andalucía.

Regulación Nacional

Código de Derecho de la Ciberseguridad *(Compendio normativo donde se puedan encontrar, actualizadas, las normas estatales que afectan directamente a la ciberseguridad. Esta recopilación incluye la normativa que se desgrana en las filas inferiores de esta sección sobre Regulación Nacional, si bien se ha considerado destacarla por su importancia).*	Código de Derecho de la Ciberseguridad actualizado
Ley 8/2011, de 28 de abril, por la que se establecen **medidas para la protección de las infraestructuras críticas.**	Ley 8-2011 Infraestructuras Criticas.pdf
Ley Orgánica 3/2018, de 5 de diciembre, de **Protección de Datos Personales y garantía de los derechos digitales.**	LOPD 3_2018.pdf
Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el **Reglamento de protección de las infraestructuras críticas.**	RD_704_2011 Protección de Infraestructuras Criticas.pdf
Real Decreto 311/2022, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad.**	Real Decreto 311-2022 Nuevo ENS.pdf
Ley 6/2020, de 11 de noviembre, **reguladora de determinados aspectos de los servicios electrónicos** de confianza	Ley 6-2020_Regul_servicios_electronicos_confianza
Ley 2/2023, de 20 de febrero, **reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción**.	Ley 2-2023-Protecc_personas_informen_infracciones
Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los **nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos**	Resolucion 8-09-2015 contenido plan seguridad operador.pdf
Resolución de 15 de noviembre de 2011, de la Secretaría de Estado de Seguridad, por la que se establecen los **contenidos mínimos de los planes de seguridad del operador y planes de protección específicos conforme a lo dispuesto en el Real Decreto 704/2011, de 20 de mayo**, por el que se aprueba el **Reglamento de protección de infraestructuras críticas.**	Resolucion 15-11-2011 contenido plan seguridad operador IC.pdf

Regulación Europea

R**EGLAMENTO (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)	RGPD_UE.pdf
REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 **relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación** y por el que se deroga el Reglamento (UE) n. o 526/2013 («Reglamento sobre la Ciberseguridad»)	Reglamento Europeo Ciberseguridad.pdf
Directiva (UE) 2022/2025 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 **relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión** por la que se modifica el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)	Directiva NIS-2.pdf
Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 **relativa a la resiliencia de las entidades críticas** y por la que se deroga la Directiva 2008/114/CE del Consejo.	Directiva RCE.pdf

REGLAMENTO (UE) 2017/745 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 5 de abril de 2017 o **sobre los productos sanitarios**, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n. 178/2002 y el Reglamento (CE) n. o 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo	REGLAMENTO-UE-2017-745.pdf
Marco de Privacidad de Datos UE-EE.UU. (11/7/2023)	• Adequacy decision EU-US Data Privacy Framework.pdf • Empresas adheridas al DPF

Instrucciones Técnicas de Seguridad, Guías y Buenas Prácticas

Instrucciones Técnicas de Seguridad (ITS)

Las **Instrucciones Técnicas de Seguridad (ITS)** dentro del Esquema Nacional de Seguridad (ENS) **son directrices detalladas que complementan los requisitos y medidas de seguridad establecidas en el ENS**. Estas ITS t**ienen como objetivo facilitar la implementación coherente y homogénea de la seguridad en los sistemas de información de la Administración Pública española.**

El Real Decreto 311/2022 establece en su disposición adicional segunda las instrucciones técnicas de seguridad, esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema Nacional de Seguridad.

Informe del Estado de la Seguridad

- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad
- Guía CCN-STIC 815 Indicadores y métricas en el ENS
- Guía CCN-STIC 824 Informe del Estado de Seguridad
- Guía CCN-STIC 844 Manual de Usuario de INES / Anexo
- Herramienta INES (Informe Nacional del Estado de Seguridad)

Conformidad con el Esquema Nacional de Seguridad

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad
- Conformidad con el Esquema Nacional de Seguridad
- Guía CCN-STIC 809 Declaración y Certificación de Conformidad con el ENS
- Guía CCN-STIC-802 Auditoría del ENS
- Guía CCN-STIC-804 ENS. Guía de implantación
- Guía CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS
- Guía CCN-STIC 824 Informe del Estado de Seguridad

Auditoría de la Seguridad de los Sistemas de Información

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Guía CCN-STIC-802 Auditoría del ENS
- Guía CCN-STIC-804 ENS. Guía de implantación

Notificación de Incidentes de Seguridad

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad
- Guía CCN-STIC-817 Gestión de Ciberincidentes

Guías CCN-CERT

Las Series CCN-STIC son **normas, instrucciones, guías y recomendaciones** desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT.

El grueso de las Series está especialmente **dirigidas al personal de las Administraciones Pública.** A continuación, se presentan las más relevantes para nuestra organización, pudiendo consultar el resto de Guías en el siguiente enlace: Índice Todas Guías CCN-STIC

200 Normas

La Serie CCN-STIC-200 comprende reglas generales que deben seguirse, o a las que se deben ajustar las conductas tareas o actividades de las personas y Organizaciones, en relación con la protección de la información cuando es manejada por un Sistema. Deben tomarse en cuenta las siguientes:

- Guía de Seguridad de las TIC CCN-STIC 201 ORGANIZACIÓN Y GESTIÓN PARA LA SEGURIDAD DE LAS TIC
- GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-205) ACTIVIDADES DE SEGURIDAD EN EL CICLO DE VIDA DE LOS SISTEMAS TIC

Guías 200 CCN-CERT-Consulta

400 Guías Generales

La Serie CCN-STIC-400 incluye recomendaciones para los responsables de seguridad relativas a aspectos concretos de la seguridad de las TIC (seguridad perimetral, redes inalámbricas, telefonía móvil, herramientas de seguridad, etc.). A tener en consideración estas: • GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-403) GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICOS • GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-412) REQUISITOS DE SEGURIDAD DE ENTORNOS Y APLICACIONES WEB • GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-422) DESARROLLO SEGURO DE APLICACIONES WEB	Guías 400 CCN-CERT-Consulta
800 Guías Esquema Nacional de Seguridad	
La Serie CCN-STIC-800 establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el Esquema Nacional de Seguridad. Las Guías publicadas con fecha anterior a mayo de 2022 (fecha de publicación del nuevo RD 311/2022), pueden no concordar con lo dispuesto en el nuevo ENS, en cuanto a requisitos de aplicación. Las Guías 808 y 807 son las primeras actualizadas a lo dispuesto en el nuevo RD 311/2022. Las más relevantes son: • Guía de Seguridad de las TIC CCN-STIC 801 ESQUEMA NACIONAL DE SEGURIDAD RESPONSABILIDADES Y FUNCIONES • Guía de Seguridad de las TIC CCN-STIC 803 Mayo 2020 ENS. Valoración de los sistemas • Guía de Seguridad de las TIC CCN-STIC 804. ENS. Guía de implantación • Guía de Seguridad de las TIC CCN-STIC 806. Plan de Adecuación al ENS • GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-812) SEGURIDAD EN ENTORNOS Y APLICACIONES WEB • Guía de Seguridad de las TIC CCN-STIC 817 Esquema Nacional de Seguridad. Gestión de ciberincidentes • Guía de Seguridad de las TIC CCN-STIC 821 ESQUEMA NACIONAL DE SEGURIDAD NORMAS DE SEGURIDAD • GUÍA DE SEGURIDAD (CCN-STIC-822) ESQUEMA NACIONAL DE SEGURIDAD PROCEDIMIENTOS DE SEGURIDAD • Guía de Seguridad de las TIC CCN-STIC 857. Requisitos de seguridad para aplicaciones de Cibersalud en el contexto del ENS • Guía CCN-STIC 891 sobre Perfil de Cumplimiento Específico para Salud y Prestación Sanitaria a Pacientes	Guías 800 CCN-CERT-Consulta
Abstracts	

Obligaciones de los prestadores de servicios a las entidades públicas	Abstract - Obligaciones Proveedores Sector Publico.pdf

Buenas Prácticas CCN-CERT

A continuación, se muestra el listado de Buenas Prácticas que CCN-CERT ha publicado y que deben tenerse en cuenta. En la columna de al lado, pueden consultarse cada una de ellas:

• Medidas de seguridad para acceso remoto • CCN-CERT BP/01. Principios y recomendaciones básicas en Ciberseguridad BP/01. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/02 Correo electrónico. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/03 . Dispositivos móviles. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/05. Internet de las Cosas. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/06. Seguridad y riesgos de los navegadores web INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/08 Buenas Prácticas en Redes Sociales. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/09. Recomendaciones de protección DoS en cortafuegos. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/10. Recomendaciones de seguridad para CDN. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/11. Recomendaciones de seguridad en redes Wi- Fi corporativas INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/12. Buenas Prácticas en Cryptojacking. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/13. Desinformación en el Ciberespacio. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/14. Declaración de Aplicabilidad en el ENS (Perfil de Cumplimiento). INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/15, AGOSTO 2021. Buenas Prácticas en Virtualización. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/16. Marzo 2022. RECOMENDACIONES DE SEGURIDAD DE ADOBE ACROBAT READER DC • CCN-CERT BP/17. Mayo 2020. RECOMENDACIONES DE SEGURIDAD DE MOZILLA FIREFOX	Consulta Documentos Buenas Prácticas CCN-CERT

• CCN-CERT BP/18. Mayo 2020. Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia • CCN-CERT BP/19. Recomendaciones de seguridad en Google Chrome. INFORME DE BUENAS PRÁCTICAS • CCN-CERT BP/20. GESTIÓN DE CIBERCRISIS BUENAS PRÁCTICAS EN LA GESTIÓN DE CRISIS DE CIBERSEGURIDAD • CCN-CERT BP/21. Gestión de incidentes de ransomware. INFORME DE BUENAS PRÁCTICAS	

Buenas Prácticas Análisis de Riesgos	
MAGERIT – versión 3.0. Metodología de Análisis y Gestión. de Riesgos de los Sistemas de Información. Libro I - Método	2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8 (1).pdf
MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos	2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8 (1).pdf
MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas	2012_Magerit_v3_libro3_guia-de-tecnicas_es_NIPO_630-12-171-8 (1).pdf