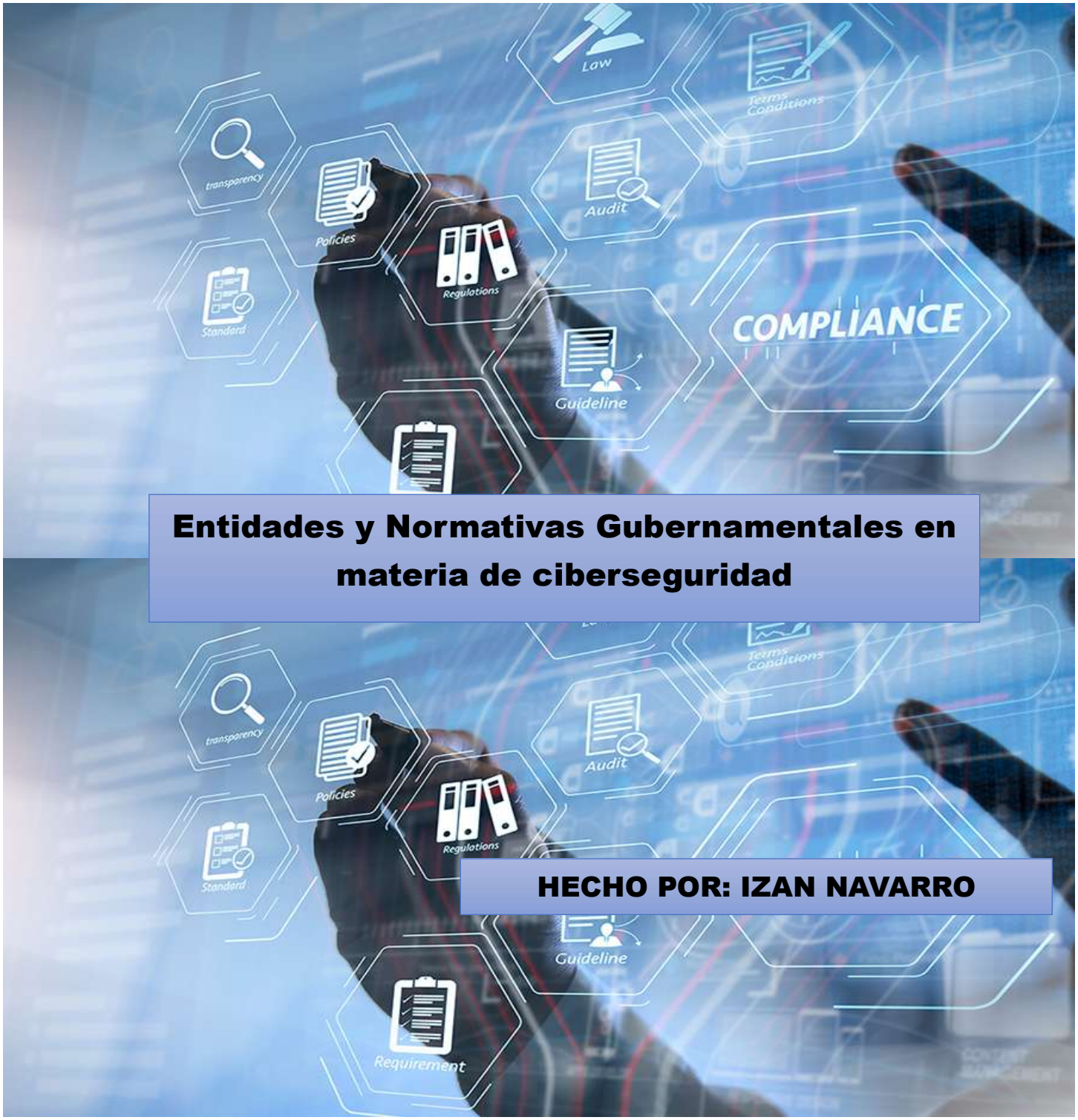


Entidades y Normativas Gubernamentales en materia de ciberseguridad

HECHO POR: IZAN NAVARRO

INDICE

1. Introducción

Como expertos de ciberseguridad hay ciertos conceptos que debemos tener muy claros. Si una empresa es afectada por un ciberataque e información sensible ha sido filtrada, por ejemplo, se tiene que notificar a las entidades oportunas.

Las entidades y normativas gubernamentales en materia de ciberseguridad son organismos y reglas establecidos por los gobiernos para proteger los sistemas, redes, y datos de las amenazas cibernéticas.

Estas entidades y normativas son esenciales para garantizar la seguridad nacional, la protección de la información sensible y la estabilidad económica. Por ello debemos conocerlas muy bien y sabemos a dónde nos tenemos que dirigir en casa de detectar algún incidente en la infraestructura.

2. Objetivos

• Conocer las principales entidades y normativas gubernamentales, tanto internacionales como nacionales, así como sus tareas principales.

• Conocer cuáles son los diferentes servicios que ofrecen estas entidades.

Las Principales entidades son:

-**INCIBE**: Instituto Nacional de Ciberseguridad, es la institución de referencia al desarrollo de la ciberseguridad como instrumento de transformación social y de la confianza digital para el público en general, RedIRIS y para empresas. Promueve formación, concienciación y captación profesional.

-**CCN-CERT:** Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional. Este es responsable de los ciberataques a sistemas y sistemas clasificados de las Administraciones Públicas y de empresas de interés estratégico.

-**CNPIC**: Centro Nacional de Protección de las Infraestructuras Críticas se creó para ser responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior.

-**NIST**: National Institute of Standards and Technology desarrolla estándares y guías en materia de seguridad de la información y proporciona metodologías para la gestión de riesgos, controles de seguridad y buenas prácticas técnicas y organizativas.

-**CISA**: Cybersecurity and Infrastructure Security Agency es la agencia federal operative encargada de proteger la infraestructura crítica de EE.UU.

Coordina respuestas a incidentes cibernéticos, emite alertas, administra programas de resiliencia/gestión de vulnerabilidades y ciberinteligencia.

-**ENISA**: European Union Agency for Cybersecurity es una agencia técnica de coordinación de ciberseguridad en EU. Esta elabora políticas, guías, buenas prácticas y marcos normativos. Coordina la cooperación entre los CSIRT europeos.

-**CCN**: Autoridad en seguridad de la información en el sector público español. Desarrolla normativa técnica que se aplica en la seguridad de la información clasificada y sensible. También supervisa la aplicación del Esquema Nacional de Seguridad (ENS).

-**ENS**: Esquema Nacional de Seguridad es el marco normativo español el cual establece principios, requisitos que deben cumplir las administraciones públicas y empresas con servicios al sector público. Define niveles de seguridad (bajo, medio, alto)

• Conocer en qué consisten las normativas en ciberseguridad, y conocer los requisitos que una empresa debe cumplir, para adaptarse a la normativa.

Las normativas en ciberseguridad son marcos legales, técnicos y organizativos que garantizan obligaciones, requisitos y buenas prácticas para proteger la información.

Su objetivo principal es:

· Garantizar la confidencialidad y disponibilidad de la información.

· Reducir riesgos tecnológicos.

· Asegurar la continuidad del negocio.

Algunas de estas normativas pueden ser:

· Internacionales; ISO/IEC, NIST Cybersecurity Framework…

· Europeas; Reglamento General de Protección de Datos (RGPD)…

· Españolas; Esquema Nacional de Seguridad (ENS)…

Todas las organizaciones deberán abordar tres pilares fundamentales: gestión, técnica y legal

1. Organizativos:

- Evaluar riesgos y activos críticos.
- Definir políticas y roles (CISO, procedimientos).
- Formar y concienciar al personal.

2. Técnicos:

- Control de accesos y privilegios mínimos.
- Protección de redes y sistemas (firewalls, antivirus, IDS/IPS).
- Gestión de vulnerabilidades y actualizaciones.

3. Legales:

- Cumplir RGPD, ENS, NIS2, DORA según corresponda.
- Mantener registros y realizar auditorías periódicas.

PRACTICA 1.1

• Elaborar un documento lo más profesional posible, con el mayor detalle, adjuntando capturas. De manera que sirva para poder explicar a la junta directiva de una empresa en qué consisten todos estos organismos y normativas

---

INFORME SOBRE ORGANISMOS Y NORMAS DE CIBERSEGURIDAD

1. Introducción:

La ciberseguridad ya no es opcional: protege datos, sistemas y la reputación de la empresa. Este informe resume **quién hace qué** y **qué normas hay que seguir** para no tener problemas.

---

2. Organismos importantes:

Internacionales / UE:

- **NIST (EE. UU.)** → hace normas y guías de seguridad.
- **CISA (EE. UU.)** → protege infraestructuras críticas y responde a incidentes.
- **ENISA (UE)** → coordina políticas y buenas prácticas en Europa.

España:

- **CCN** → normas de seguridad para el sector público.
- **CCN-CERT** → responde a incidentes en la administración.
- **INCIBE** → protege empresas y ciudadanos, maneja su propio CERT.
- **CNPIC** → cuida infraestructuras críticas.
- **ENS** → marco obligatorio de seguridad para la administración.

---

3. Normas clave

- **Internacional:** ISO 27001 (SGSI), NIST Framework.
- **Europeas:** RGPD (datos personales), NIS2 (operadores esenciales), DORA (sector financiero).
- **España:** ENS, Ley 8/2011 y RD 311/2022 (infraestructuras críticas), LOPDGDD (adaptación del RGPD).

ens
Esquema Nacional de Seguridad

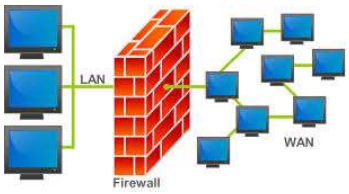
---

4. Qué debe hacer la empresa

Organizativo:

- Evaluar riesgos, definir políticas y roles (CISO), formar al personal.

Técnico:



- Control de accesos, firewalls, antivirus, parches, cifrado, backups, monitorización.

Legal:

- Cumplir RGPD, ENS, NIS2 o DORA según corresponda.
- Notificar incidentes y mantener registros.
- Hacer auditorías periódicas.

---

5. Ejemplo práctico

Si tu empresa trabaja con la administración pública:

1. Cumple ENS (nivel medio/alto).
2. Pon cifrado, MFA y backups.
3. Aplica RGPD para los datos de ciudadanos.
4. Forma al personal y haz auditorías.
5. Notifica incidentes al CCN-CERT.

---

6. Conclusión

La ciberseguridad es estratégica, no solo para evitar sanciones, sino para **proteger información crítica y mantener la confianza de clientes y socios**.

3. Bibliografía

https://ciberseguridad.com/normativa/espana/organismos