XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas

RGPD y ENS:
dos caminos convergentes

CCN-CERT
centro criptológico nacional

Dr. Carlos Galán

Licenciado y Doctor en Informática, Licenciado en Derecho y Abogado especialista en Derecho de las TIC.

Profesor de la Universidad Carlos III de Madrid, asesor del CCN-CERT y miembro del Grupo de Trabajo de Ciberpolíitica del Real Instituto Elcano.

cgalan@der-pu.uc3m.es / cgalan@atl.es

Índice

El RGPD y el ENS son –probablemente- las dos normas de obligado cumplimiento que más van a impactar en el desenvolvimiento digital de las entidades del Sector Público…

… y nos hacemos algunas preguntas:

- ¿Hay algún punto de convergencia entre ambas regulaciones?
- ¿Pueden compaginarse los esfuerzos que requiere alcanzar su conformidad?
- ¿Caben sinergias, aproximaciones conjuntas, combinadas…?

ENS
RD 3/2010

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

ENS

Preceptos de cumplimiento
(de sustrato jurídico y organizativo)

- Gestión de la seguridad basada en riesgos.
- La seguridad como función diferenciada.
- Seguridad por defecto.
- Certificación de conformidad.
- Etc.

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

ENS

Preceptos de cumplimiento
(de sustrato jurídico y organizativo)

Medidas de Seguridad
(de sustrato tecnológico)

- Gestión de la seguridad basada en riesgos.
- La seguridad como función diferenciada.
- Seguridad por defecto.
- Certificación de conformidad.
- Etc.

- Anexo II

- Gestión de la seguridad basada en riesgos.
- La seguridad como función diferenciada.
- Seguridad por defecto.
- Certificación de conformidad.
- Etc.

- Anexo II

ENS

Preceptos de cumplimiento
(de sustrato jurídico y organizativo)

Medidas de Seguridad
(de sustrato tecnológico)

ANÁLISIS DE RIESGOS

RGPD (2016)

PROTECCIÓN DE LOS DERECHOS Y LIBERTADES

ENS

- Principios relativos al tratamiento.
- Condiciones para el consentimiento.
- Categorías especiales de datos.
- Delegado de Protección de Datos.
- Etc.

Medidas de Seguridad
(de sustrato tecnológico)

ANÁLISIS DE RIESGOS

RGPD

Preceptos de cumplimiento
(de sustrato jurídico y organizativo)

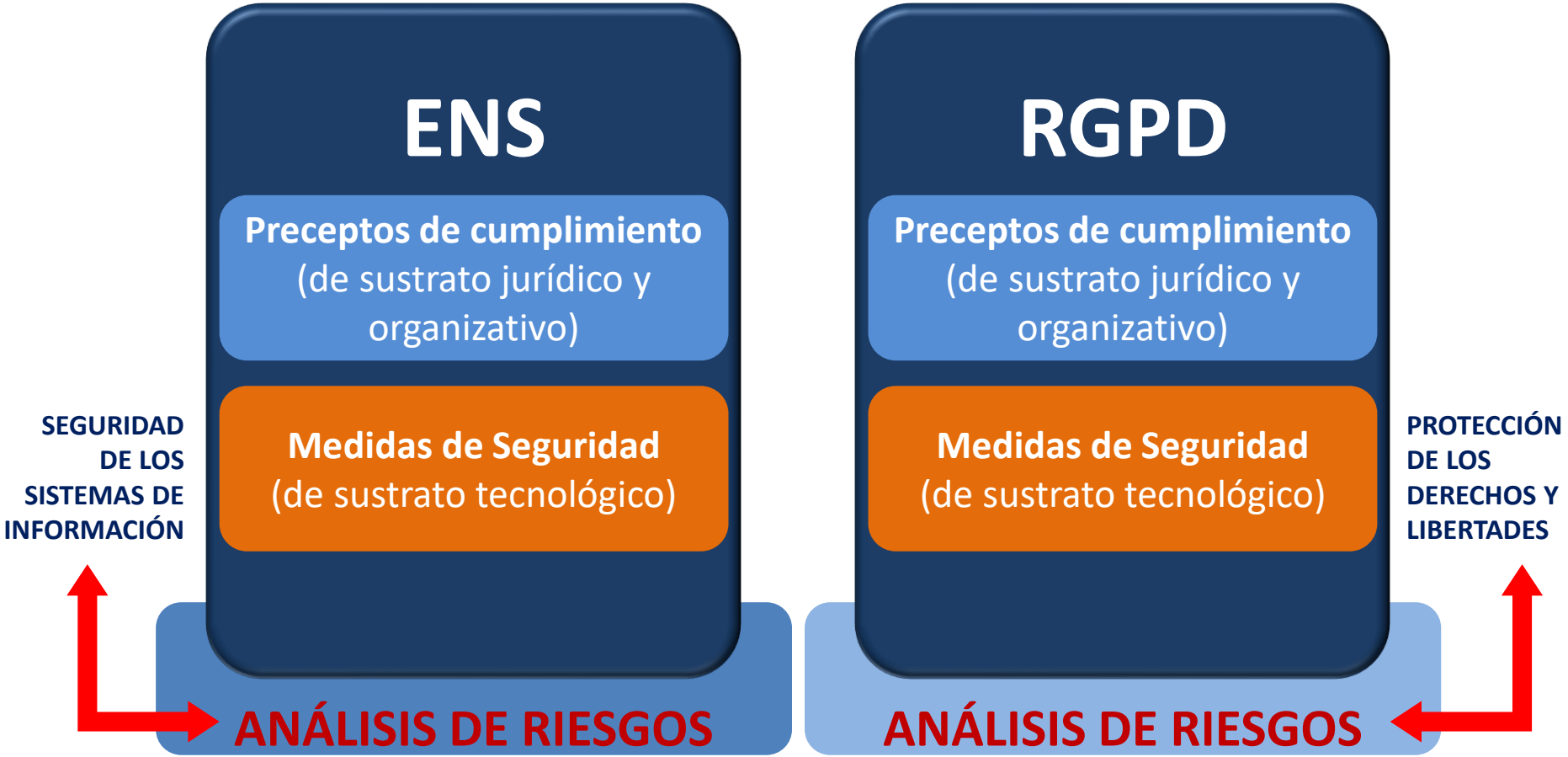
PROTECCIÓN DE LOS DERECHOS Y LIBERTADES

- Principios relativos al tratamiento.
- Condiciones para el consentimiento.
- Categorías especiales de datos.
- Delegado de Protección de Datos.
- Etc.

- Exigencia de medidas técnicas.

PROTECCIÓN DE LOS DERECHOS Y LIBERTADES


ENS
• Principios relativos al tratamiento.
• Condiciones para el consentimiento.
• Categorías especiales de datos.
• Delegado de Protección de Datos.
• Etc.
Medidas de Seguridad
• Medidas técnicas.
ANÁLISIS DE RIESGOS
RGPD
Preceptos de cumplimiento
(de sustrato jurídico y organizativo)
Medidas de Seguridad
(de sustrato tecnológico)
ANÁLISIS DE RIESGOS
PROTECCIÓN DE LOS DERECHOS Y LIBERTADES


ENS
Preceptos de cumplimiento (de sustrato jurídico y organizativo)
Medidas de Seguridad (de sustrato tecnológico)
RGPD
Preceptos de cumplimiento (de sustrato jurídico y organizativo)
Medidas de Seguridad (de sustrato tecnológico)
SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
PROTECCIÓN DE LOS DERECHOS Y LIBERTADES
ANÁLISIS DE RIESGOS
ANÁLISIS DE RIESGOS

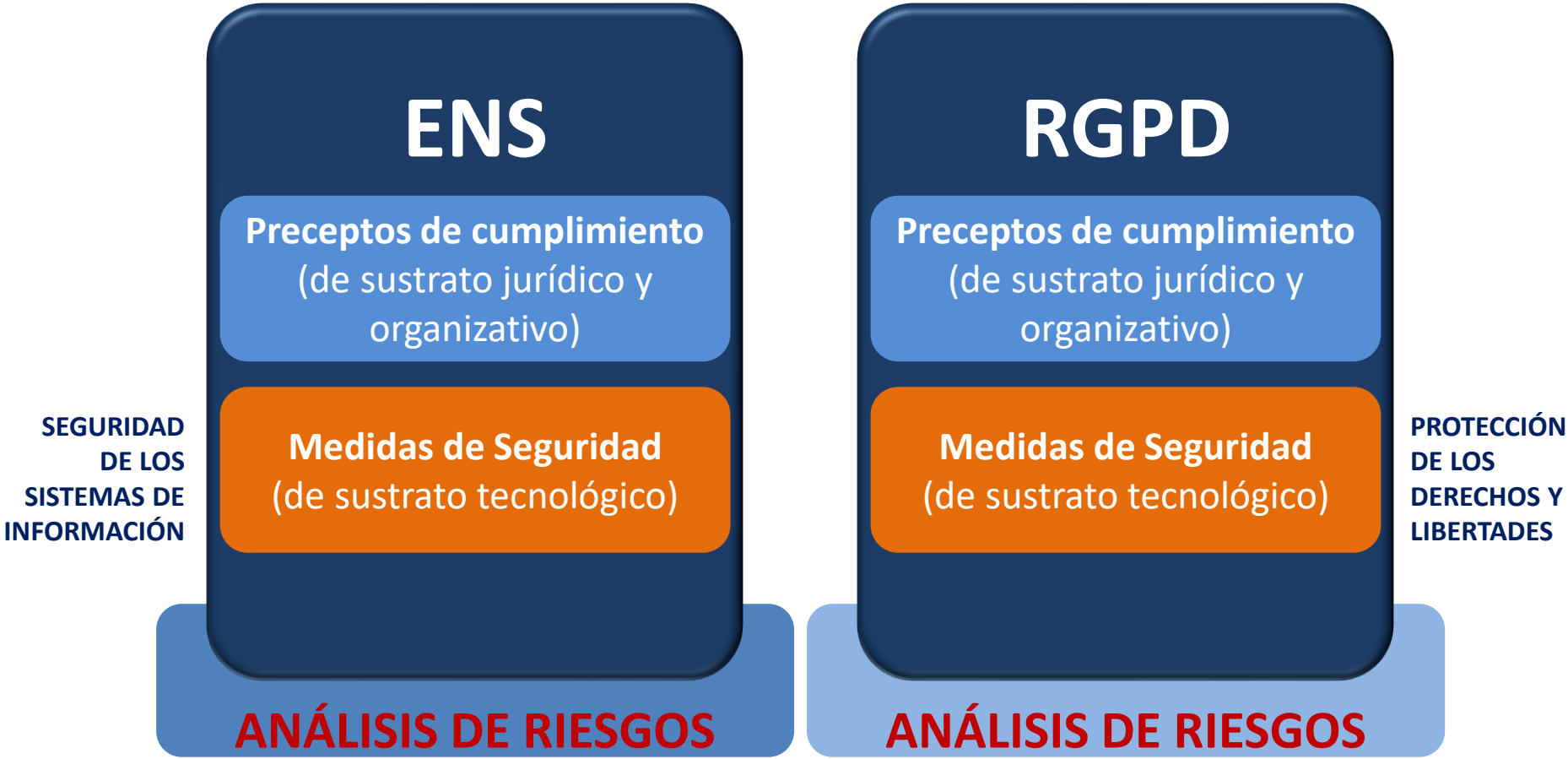
LEY ORGÁNICA 3/2018 DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

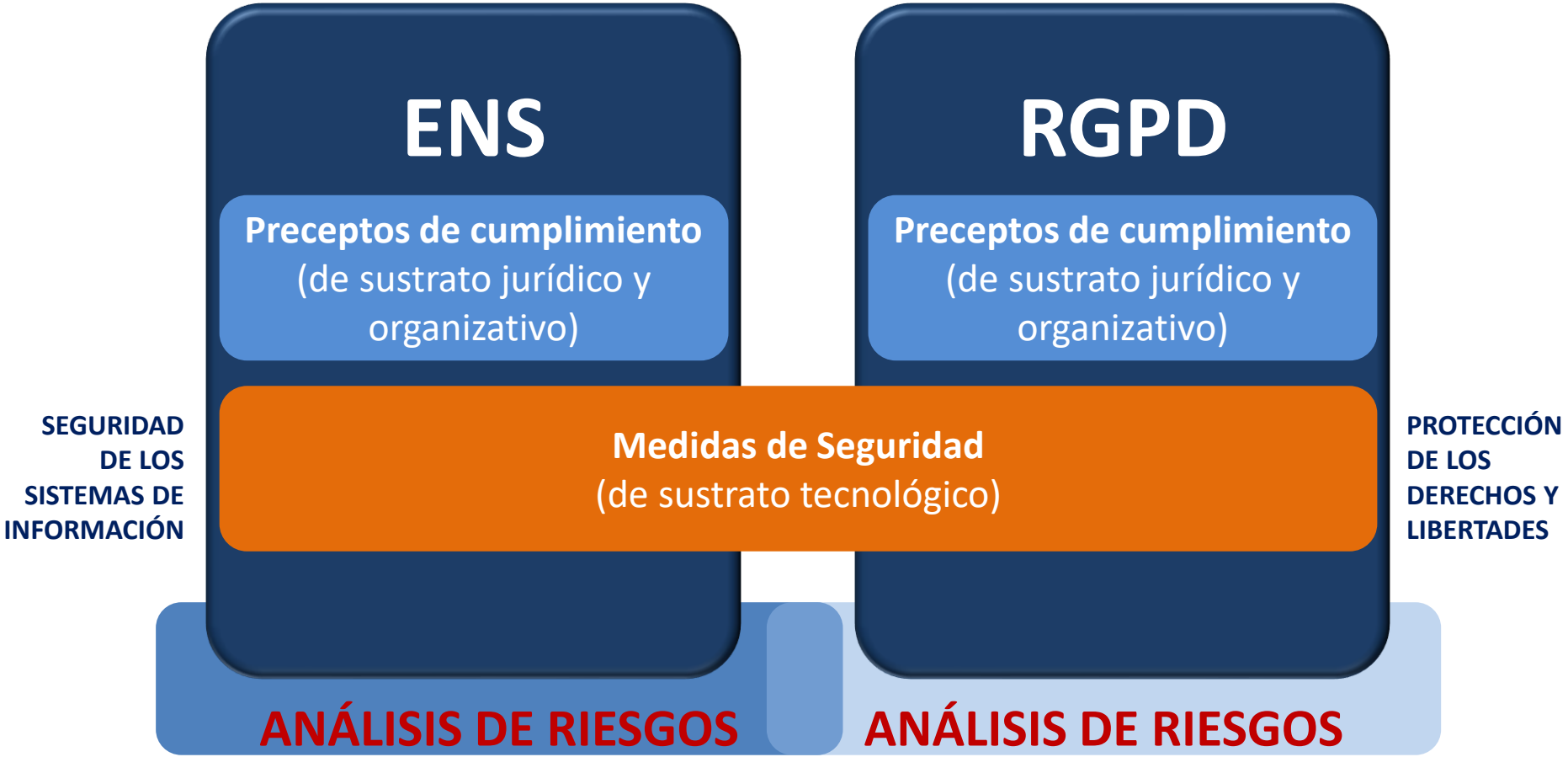
Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.

1. **El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse 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.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán **aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad**, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un **servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad**.


ENS
Preceptos de cumplimiento (de sustrato jurídico y organizativo)
Medidas de Seguridad (de sustrato tecnológico)
ANÁLISIS DE RIESGOS
RGPD
Preceptos de cumplimiento (de sustrato jurídico y organizativo)
Medidas de Seguridad (de sustrato tecnológico)
ANÁLISIS DE RIESGOS
SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
PROTECCIÓN DE LOS DERECHOS Y LIBERTADES


ENS
Preceptos de cumplimiento
(de sustrato jurídico y organizativo)
RGPD
Preceptos de cumplimiento
(de sustrato jurídico y organizativo)
SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
Medidas de Seguridad
(de sustrato tecnológico)
PROTECCIÓN DE LOS DERECHOS Y LIBERTADES
ANÁLISIS DE RIESGOS
ANÁLISIS DE RIESGOS

Ambas regulaciones (RGPD y ENS) exigen demostrar conformidad.

En el caso del ENS, además, la conformidad se evidencia en base a las Certificaciones de Conformidad de su Esquema de Certificación, mediante Auditorías periódicas.

Así las cosas…

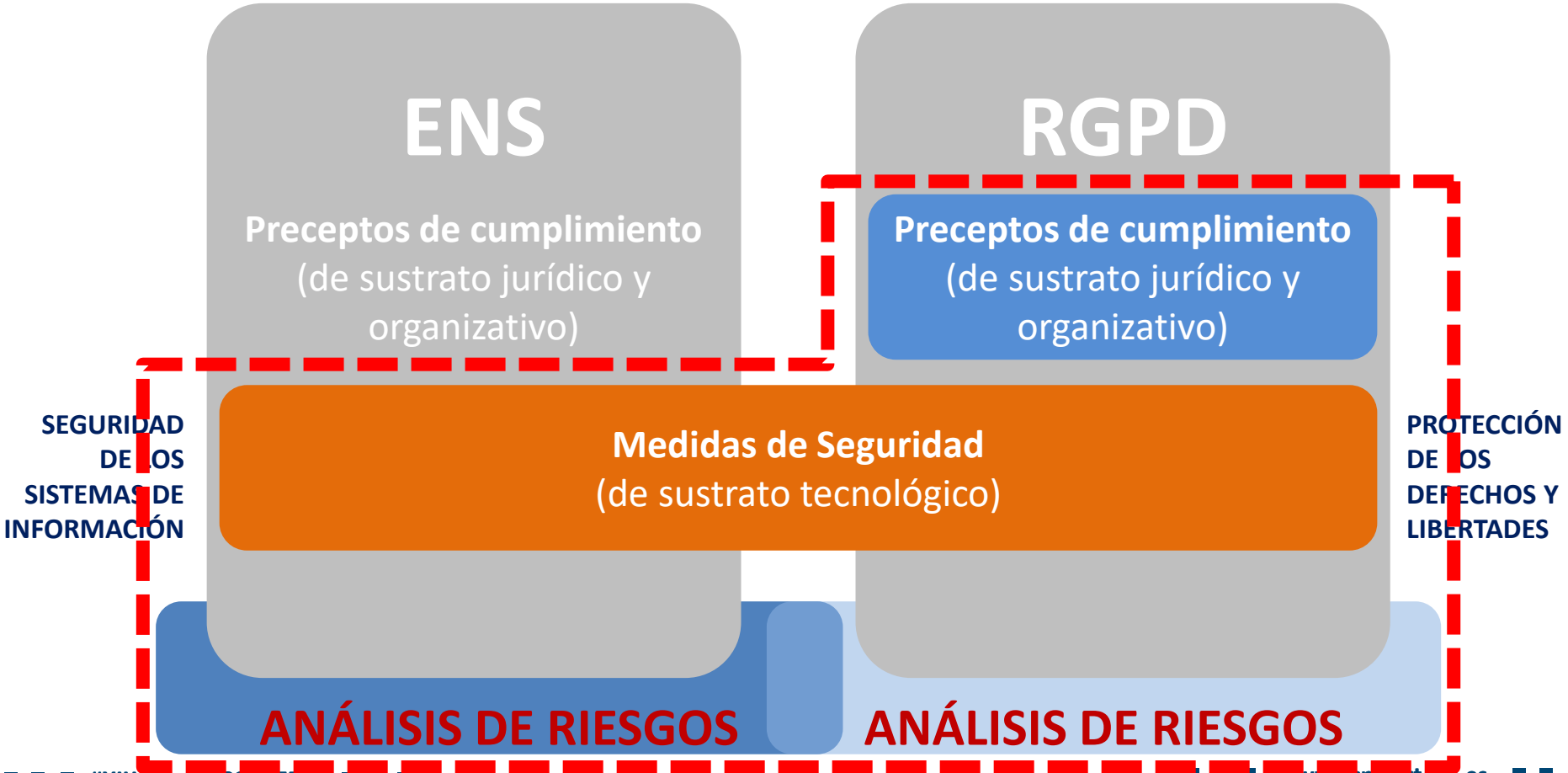
¿Qué podemos/debemos hacer ahora para optimizar los esfuerzos de conformidad?

Así las cosas…

¿Qué podemos/debemos hacer ahora para optimizar los esfuerzos de conformidad?

Aprovechar lo que tenemos…

… y completar lo que nos falta.


ENS
Preceptos de cumplimiento
(de sustrato jurídico y organizativo)
RGPD
Preceptos de cumplimiento
(de sustrato jurídico y organizativo)
SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
Medidas de Seguridad
(de sustrato tecnológico)
PROTECCIÓN DE LOS DERECHOS Y LIBERTADES
ANÁLISIS DE RIESGOS
ANÁLISIS DE RIESGOS

Guía CCN-STIC 881 Impacto del RGPD en el ENS

El **objetivo** de esta Guía es examinar el impacto del RGPD (y la LOPDGDD) en el ENS y contribuir a sentar las bases para el desarrollo de un **MODELO DE EVALUACIÓN COMBINADO RGPD-ENS** que facilite a las entidades del Sector Público del ámbito de aplicación simultánea de ambas regulaciones, los requisitos de evaluación y, en su consecuencia, permita la obtención de las adecuadas evidencias de conformidad.

Guía CCN-STIC 881 - (CONCEPTOS ANALIZADOS)

1. BASE JURÍDICA DEL TRATAMIENTO
2. UTILIZACIÓN DE MEDIOS ELECTRÓNICOS
3. POLÍTICA DE PROTECCIÓN DE DATOS – POLÍTICA DE SEGURIDAD
4. INTERCONEXIÓN DE REDES
5. FUENTE (SELLOS) DE TIEMPO
6. RESPONSABLE DEL TRATAMIENTO Y ENCARGADO DEL TRATAMIENTO
7. ENCARGADOS DE TRATAMIENTO – SERVICIOS EXTERNOS
8. MECANISMOS DE CERTIFICACIÓN - CERTIFICACIONES (DE CONFORMIDAD)
9. SELLOS Y MARCAS DE PROTECCIÓN DE DATOS – DISTINTIVOS DE CONFORMIDAD

10. PROVEEDORES DE PRODUCTOS O SERVICIOS (DE SEGURIDAD)
11. CATEGORIAS ESPECIALES DE DATOS PERSONALES - CATEGORIZACIÓN DE SISTEMAS
12. ANÁLISIS DE RIESGOS – EVALUACIÓN DE IMPACTO
13. REGISTRO DE ACTIVIDAD DE LOS USUARIOS – MONITORIZACIÓN
14. MEDIDAS DE SEGURIDAD (TÉCNICAS Y ORGANIZATIVAS)
15. NOTIFICACIÓN DE VIOLACIONES (BRECHAS) DE SEGURIDAD – NOTIFICACIÓN DE CIBERINCIDENTES
16. DELEGADO DE PROTECCIÓN DE DATOS – RESPONSABLE DE SEGURIDAD DEL ENS

ELEMENTOS (Ejemplo):

Concepto analizado (y epígrafe de este documento)	**Ubicación en el RGPD**	**Ubicación en la LOPDGDD**	**Referencia en el ENS**	**Respuesta**
3. Base jurídica del tratamiento	Considerandos 10, 40, 45, 51 y 65 Artículo 6	Artículo 8	Artículo 1	Las medidas para tratar el impacto no exigen modificar el ENS más allá del nuevo conjunto de controles relativos a la evaluación de la conformidad con el RGPD (y LOPDGDD) que se señalan en el epígrafe 16.
4. Utilización de medios electrónicos	Considerandos 59 y 141 Artículos 12, 15 y 28	Artículos 11, 31, 38 y DA17	Artículos 31 y 33 Medidas 4.2.1, 4.2.5, 4.2.7 y 5.7.4	Las medidas para tratar el impacto no exigen modificar el ENS.
5. Política de Protección de Datos - Política de Seguridad	Considerando 78 Artículo 24	Artículos 28 y 33	Artículo 11	Es necesario incluir un nuevo párrafo 4 al art. 11 del ENS.
6. Interconexión de redes	Artículo 60, 61, 64, 67 y 75	Artículos 38 y 58	Art. 22 Medidas 4.1.2, 4.2 y 5.4.4 ITS de Interconexión en el ENS	Las medidas para tratar el impacto no exigen modificar el ENS.
7. Fuente (sellos) de tiempo	Considerando 59 Artículo 12	Arts. 16 y 41	Artículo 33 Medida 5.7.5	Las medidas para tratar el impacto no exigen modificar el ENS.
8. Responsable del Tratamiento y Encargado del Tratamiento	Numerosos Considerandos y Artículos Artículos 4 y 26	Numerosos Considerandos y Artículos Artículos 28, 29 y 33	Artículo 10	Nueva redacción al art. 10 del ENS.

(55) CONTROLES (ADICIONALES) DE CONFORMIDAD. Ejemplo:

Ref. Control PD	Control (Aspecto a evaluar)	Objetivo perseguido por el control	Preceptos del RGPD a evaluar	Medida(s) del ENS de referencia, soporte o ayuda a la conformidad con el RGPD
[pd.15]	Derecho de acceso del interesado	Asegurar que el responsable del tratamiento posibilita al interesado el ejercicio de su derecho a obtener confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la información señalada en el RGPD.	Art. 15	Medidas [org.2] y [org.3] en relación con la redacción y aprobación de Normas y Procedimientos específicos en materia de ejercicio de derechos. Medidas [op.acc] y [mp.info.4], en relación con la identificación del interesado. Anexo II (en relación con el art. 15.3)

CONCLUSIONES

El desarrollo de un **Modelo de Evaluación Combinado RGPD-ENS** reporta importantes **beneficios:**

- Mayor eficiencia de los recursos utilizados para alcanzar la conformidad legal: humanos, materiales y económicos.
- Impulsa el cumplimiento normativo del RGPD y del ENS

Y siempre respetando las peculiaridades de cada norma y cada bien jurídico protegido.

Muchas gracias.

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional