XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas



Cumplimiento integrado ENS-RGPD en el Gobierno Vasco – Eusko Jaurlaritza

CCN-CERT
centro criptológico nacional



Xabier Arrieta

Eusko Jaurlaritza – Gobierno Vasco
Director de Informática y Telecomunicaciones

jr-suso@euskadi.eus



Joseba Enjuto

S21Sec | Nextel

Head of Consulting Department

jenjuto@nextel.es

Índice

1. Situación de partida

2. El proyecto de adecuación al RGPD

3. Cumplimiento integrado ENS-RGPD

4. Visión de futuro

5. Conclusiones

Índice

1. Situación de partida

- Dirección de Informática y Telecomunicaciones del GV —DIT—
- Sociedad Informática del GV —EJIE—
- Gestión de la Seguridad de la Información en el Gobierno Vasco

2. El proyecto de adecuación al RGPD

3. Cumplimiento integrado ENS-RGPD

4. Visión de futuro

5. Conclusiones

Situación de partida

La Dirección de Informática y Telecomunicaciones (DIT)



Situación de partida

La Sociedad Informática del Gobierno Vasco (EJIE)

Somos EJIE

EJIE es la Sociedad Informática del Gobierno Vasco que a través del liderazgo tecnológico facilita la digitalización de los servicios que el Sector Público Vasco presta a la ciudadanía para un mejor y más eficiente cumplimiento de sus objetivos.

EJIE desarrolla su actividad en el amplio campo de las Tecnologías de la Información y Telecomunicaciones, para lo que cuenta con recursos e infraestructuras, que avalan la prestación de los Servicios y la oferta de Productos que se describen en este apartado, con las máximas garantías de Calidad, Eficiencia y Seguridad.



Desarrollo de proyectos



Consultoría y asistencia técnica



Infraestructura y explotación



Otros servicios

Situación de partida

La Sociedad Informática del Gobierno Vasco (EJIE)

- Infraestructura y Explotación
  - Albergue – Housing – CPDs
  - Comunicaciones y seguridad
  - Explotación
  - Puesto de persona usuaria a toda Administración autonómica
  - Servicios
- Consultoría y Asistencia Técnica
- Desarrollo de proyectos

Situación de partida

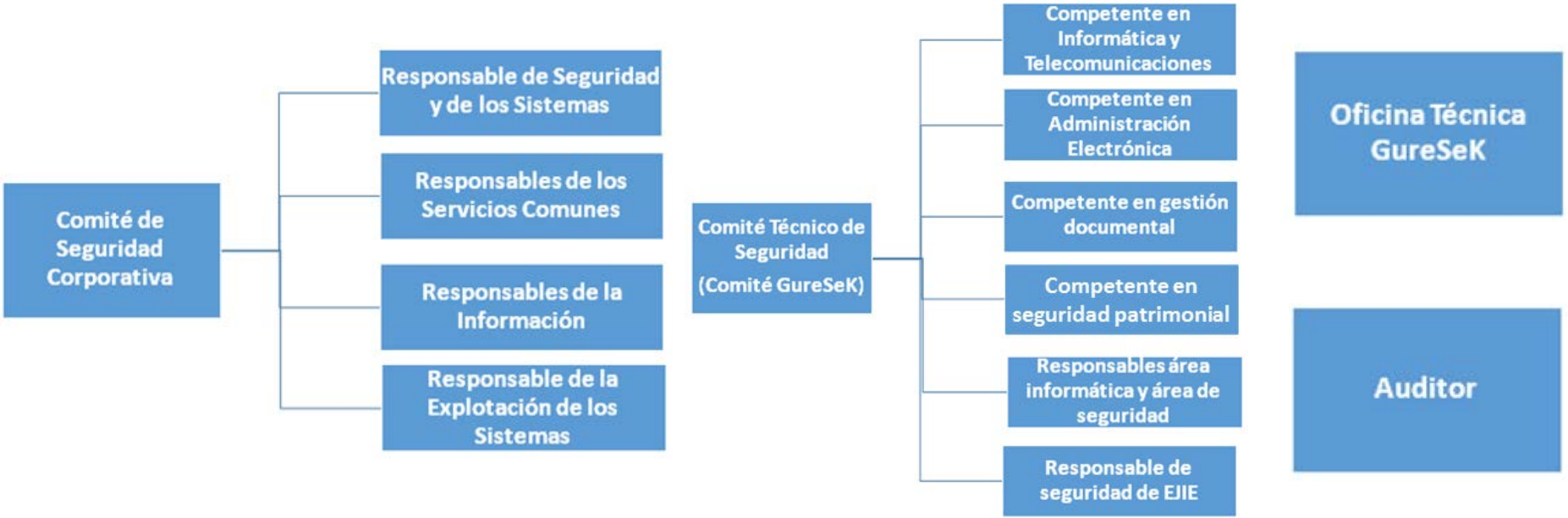
Gestión de la Seguridad de la Información en el Gobierno Vasco

- Marco general ENS regulado en:
  - «***Acuerdo de Consejo de Gobierno, de 30 de junio de 2015, por el que se aprueba la estructura organizativa y asignación de roles de seguridad para la Administración Electrónica del Gobierno Vasco (exp. 2015/00436) (A/20150120)***».

Situación de partida

Gestión de la Seguridad de la Información en el Gobierno Vasco

- Estructura organizativa:



Situación de partida

Gestión de la Seguridad de la Información en el Gobierno Vasco

- Marco regulatorio
  - Política de Seguridad:
    - En la Sede electrónica del GV



  - Normativa aplicable:
    - PLATEA: Manual de Seguridad
    - Obligaciones generales para las personas usuarias
    - Guía de recomendaciones para un uso seguro de los dispositivos y de las redes sociales



Situación de partida

Gestión de la Seguridad de la Información en el Gobierno Vasco

- Marco de gestión: Proceso GureSeK (Gure Segurtasun Kudeaketa)



Situación de partida

Gestión de la Seguridad de la Información en el Gobierno Vasco

- Modelo de Gestión: GV + EJIE
  - Anexo al Encargo General, con delimitación de responsabilidades

CÓDIGO	MEDIDA DE SEGURIDAD	Reparto Responsabilidades	
		Responsabilidad de GV	Responsabilidad de EJIE
C:org	Marco organizativo		
GENERAL	Funciones y Responsabilidades	100%	0%
C:org.1	Política de Seguridad	100%	0%
C:org.2	Normativa de seguridad	100%	0%
C:org.3	Procedimientos de seguridad	50%	50%
C:org.4	Proceso de autorización	50%	50%
C:op	Marco operacional		
C:op.pl	Planificación		
C:op.pl.1	Análisis de riesgos	80%	20%
C:op.pl.2	Arquitectura de seguridad	20%	80%
C:op.pl.3	Adquisición de nuevos componentes	10%	90%
C:op.pl.4	Dimensionamiento / Gestión de capacidades	0%	100%
C:op.pl.5	Componentes certificados	10%	90%
C:op.acc	Control de acceso		
C:op.acc.1	Identificación	20%	80%
C:op.acc.2	Requisitos de acceso	20%	80%

Situación de partida

Gestión de la Seguridad de la Información en el Gobierno Vasco

- Gestión madura
  - Resultados Informe INES CC.AA. 2017:

Organismo	Índice de Madurez	Índice de Cumplimiento
2017 Gobierno Vasco	83,07	86,81

Índice

1. Situación de partida

2. El proyecto de adecuación al RGPD
- Fase 1: *finales de 2017*
- Fase 2: *principios de 2018*

3. Cumplimiento integrado ENS-RGPD

4. Visión de futuro

5. Conclusiones

El proyecto de adecuación al RGPD

Fase 1 (2017)

- Análisis interno
  - Debate en Consejo de Gobierno
  - Se encarga su impulso al Departamento de Gobernanza Pública y Autogobierno
  - Se crea un equipo de trabajo con la participación de:
    - Viceconsejera de Administración y Servicios Generales
    - DIT (Viceconsejería de Administración y Servicios Generales)
    - Dirección de Función Pública (Viceconsejería de Función Pública)
    - Dirección de Desarrollo Legislativo (Viceconsejería de Régimen Jurídico)
    - Agencia Vasca de Protección de Datos

El proyecto de adecuación al RGPD

Fase 1 (2017)

- Contratación de Oficina Técnica
  - Objetivos:
    - Proporcionar un servicio de asistencia técnica a la implantación del RGPD en el Gobierno Vasco
      - Soporte especializado
      - Asesoramiento
      - Apoyo instrumental
    - Realizar las labores de gestión asociadas a la Secretaría Técnica
  - Adjudicatarios:

S21sec Nextel S.A. + DAYNTIC LEGAL

El proyecto de adecuación al RGPD

Fase 1 (2017)

- Resultados Oficina Técnica
  - Secretaría Técnica
    - Contraste externo: AEPD, CCN, avances en otras administraciones
    - Interlocución con AVPD
    - Encuestas: dinamización interna
  - Asesoría técnica
    - Revisión de documentación previa (ENS / LOPD)
    - Adaptación del Encargo general a EJIE
    - Desarrollo de nuevas propuestas

El proyecto de adecuación al RGPD

Fase 1 (2017)

- Resultados Oficina Técnica

  Propuesta de alternativas de modelo organizativo, destacando:



El proyecto de adecuación al RGPD

Fase 1 (2017)

- Resultados Oficina Técnica
  - Modificaciones documentales:
    - Desaparece el «*Documento de Seguridad*»
    - Se amplía el marco de actuación de la documentación de **seguridad** para considerar también la **privacidad**
    - Se modifica el «*Anexo de protección de datos*» del Encargo general a EJIE
    - Se crea nueva documentación, entre la que destaca:
      - Procedimiento de Gestión del Registro de Tratamientos
      - Guía de Evaluación de Impactos

El proyecto de adecuación al RGPD

Fase 2 (2018)

- Análisis interno
  - Se debaten las alternativas de modelo organizativo
    - Dentro del equipo de trabajo
  - Se define el modelo organizativo final (I)
    - **Decreto 7/2018** → Incorpora la supervisión interna de la observancia del RGPD al *Departamento de Gobernanza Pública y Autogobierno*
    - **Decreto 81/2018** → Adscribe a la *Viceconsejería de Régimen Jurídico*, sin integrarse en su estructura jerárquica, al delegado o delegada de protección de datos de la Administración Pública de la Comunidad Autónoma de Euskadi
      - Con consideración de alto cargo y rango o categoría asimilada a la de Director/a
      - Nombrada por el Consejo de Gobierno por un período de 6 años
      - Inamovible salvo renuncia o negligencia grave

El proyecto de adecuación al RGPD

Fase 2 (2018)

- Análisis interno
  - Se define el modelo organizativo final (II)
    - **Decreto 83/2018** → Se nombra a la **Delegada de Protección de Datos** de la Administración Pública de la Comunidad Autónoma de Euskadi
    - **Acuerdo de Consejo de Gobierno, de 19 de junio** → Se aprueba la estructura organizativa y asignación de roles para la protección de los datos personales tratados por la Administración Pública de la Comunidad Autónoma de Euskadi

El proyecto de adecuación al RGPD

Fase 2 (2018)

- Contratación de nueva Oficina Técnica:
  - Objetivos:
    - Puesta en marcha de las propuestas y conclusiones previas
    - El asesoramiento para el despliegue del modelo de roles y responsabilidades
    - El desarrollo del documento legal que corresponda para dar forma al marco de gestión del RGPD
    - Las labores de gestión asociadas al Plan de Adecuación
  - Adjudicatarios:

S21sec Nextel S.A. + DAYNTIC LEGAL

El proyecto de adecuación al RGPD

Fase 2 (2018)

- Resultados nueva Oficina Técnica (I)
  - Diseño final del marco organizativo



El proyecto de adecuación al RGPD

Fase 2 (2018)

- Resultados nueva Oficina Técnica (II)
  - Soporte para el desarrollo de los instrumentos legales anteriormente citados
  - Diseño final de los mecanismos de soporte al cumplimiento del RGPD
    - Política de Privacidad
    - Registro de Actividades de Tratamiento
    - Documentación operativa
  - Desarrollo del proceso para el cumplimiento integrado ENS-RGPD

Índice

1. Situación de partida

2. El proyecto de adecuación al RGPD

3. Cumplimiento integrado ENS-RGPD
- El marco organizativo
- El marco normativo
- El modelo operativo

4. Visión de futuro

5. Conclusiones

El proyecto de adecuación al RGPD

El marco organizativo

- Roles unipersonales (I)
  - Directores sectoriales
    - Responsables de los tratamientos (RGPD)
    - Responsables de los servicios comunes (ENS)
      - Administración Electrónica y Presencia en Internet
      - Gestión de la información geográfica
      - Gestión de la seguridad patrimonial
      - Gestión documental
      - Gestión de personal
      - Gestión económica
  - Directores de Servicios o asimilados de cada Departamento / Organismo Autónomo / Ente Público de Derecho Privado
    - Responsables de la información (ENS)
    - Responsables de las medidas de privacidad (RGPD)

El proyecto de adecuación al RGPD

El marco organizativo

- Roles unipersonales (II)
  - Director de la DIT
    - Responsable de la Seguridad y de los Sistemas (ENS)
  - Delegada de Protección de Datos
    - Delegada de Protección de Datos (RGPD)
  - Personal de la Dirección de Servicios (o asimilada) de cada Departamento / OA / EPDP
    - Referente de Protección de Datos (RGPD)
  - EJIE
    - Responsable de la explotación de los sistemas (ENS)
    - Encargado principal del tratamiento (RGPD)

El proyecto de adecuación al RGPD

El marco normativo

- Políticas
  - Política de Seguridad (pública)
  - Política de Privacidad (Pdte. publicar)
    - Política marco, «espejo» de la de seguridad
- Normas
  - Manual de Seguridad PLATEA
    - Desarrollo normativo



El proyecto de adecuación al RGPD

El marco normativo

- Obligaciones
  - Obligaciones generales para las personas usuarias
    - Ampliado (Pdte. publicar)
      - Nuevo apartado «tratamiento de datos personales»

El proyecto de adecuación al RGPD

El marco operativo

- Registro de actividades de tratamiento
  - Gobierno Vasco dispone de un Catálogo de Servicios (CdS)
    - Base para el análisis de servicios del ENS
    - Recoge servicios externos e internos
  - Se decide considerar Servicio (e-Admon./ENS) = Tratamiento (RGPD)
    - Se incorporarán en la herramienta los campos complementarios necesarios
  - Se desarrolla la documentación complementaria para su uso
    - Guía de gestión del registro de tratamientos (interno)

El proyecto de adecuación al RGPD

El marco operativo

- Análisis de riesgos
  - El GV dispone de un análisis de riesgos de seguridad por servicio (ENS)
    - Soportado por herramienta *GlobalSuite*
    - Integrado con la herramienta del *CdS*
  - Se decide integrar el análisis de riesgos de privacidad en el ya existente
    - Se incorporan nuevos criterios a valorar desde el punto de vista de la Privacidad
    - Se calcula un nivel de impacto (B/M/A) para la nueva dimensión de Privacidad
      - Se completa el análisis de riesgos de manera integrada (seguridad-privacidad)
  - Se actualiza la documentación complementaria para su uso
    - Metodología de análisis de riesgos (interno)

El proyecto de adecuación al RGPD

El marco operativo

- Medidas de privacidad
  - Se elimina el «*Documento de Seguridad*»
    - La regulación de la privacidad se integra con la regulación de la seguridad (ENS)
  - Se desarrollan documentos específicos para regular aspectos concretos de la privacidad
    - Protocolo para articular los ejercicios de derechos de los interesados (interno)
    - Guía sobre transparencia e información (interno)
    - Metodología para la ejecución de Evaluaciones de Impacto en la Privacidad (interno)

El proyecto de adecuación al RGPD

El marco operativo

- Medidas de seguridad
  - Se actualiza la documentación de seguridad para integrar la privacidad
    - Procedimiento de administración de usuarios y accesos (interno)
    - Guía de seguridad y privacidad de compras (interno)
    - Procedimiento de gestión de incidentes de seguridad (interno)
    - Política de auditorías (interno)
  - Se desarrollan documentos específicos para regular aspectos concretos de la privacidad
    - Procedimiento de ejercicio de derechos (interno)
    - Guía sobre transparencia e información (interno)

El proyecto de adecuación al RGPD

El marco operativo

- Medidas de seguridad
  - Se actualiza el «*Anexo de Protección de Datos*» del Encargo general a EJIE
    - Se define un marco general de niveles de seguridad a aplicar en función de los requisitos de privacidad
    - El modelo de relación requerirá sólo de la indicación del nivel requerido por cada encargo de tratamiento

Índice

1. Situación de partida

2. El proyecto de adecuación al RGPD

3. Cumplimiento integrado ENS-RGPD

4. Visión de futuro

5. Conclusiones

Visión de futuro

Tareas pendientes

- Transversales
  - Liberación de la nueva versión del *CdS*

- Por Departamento / Organismo Autónomo / EPDP
  - Formalización «*legal*» de los tratamientos
    - Desarrollo y aplicación de las cláusulas
    - Desarrollo y aplicación de contratos
  - Cumplimentación de los nuevos campos requeridos en el *CdS*
  - Aplicación práctica de la documentación desarrollada

Visión de futuro

Mejoras previstas

- Internas
  - Optimización del proceso **GureSeK,** en su apartado de privacidad
    - Declaración de aplicabilidad dual (seguridad / privacidad)
    - Indicadores específicos de privacidad
    - Reporting dual (seguridad / privacidad)
  - Depuración de los mecanismos de auditoría
    - Auditorías integradas ENS / RGPD
- Con visibilidad externa
  - Certificación ENS
  - Certificación RGPD

Índice

1. Situación de partida

2. El proyecto de adecuación al RGPD

3. Cumplimiento integrado ENS-RGPD

4. Visión de futuro

5. Conclusiones

Conclusiones

Integrar ENS y RGPD es un factor clave

- Permite ahorrar esfuerzos
- Confiere una visión de la privacidad en forma de Proceso
  - Mejora continua
- Garantiza una gestión integrada de la seguridad (de la información y los datos)

Conclusiones

Un buen punto de partida es fundamental

- Permite tiempos de adecuación moderados
  - 6-9 meses en una administración del tamaño del Gobierno Vasco
- Permite costes reducidos en consultoría especializada
  - Dentro del actual umbral “súper-simplificado”
- Permite acotar la dedicación interna necesaria
  - Abordar sólo la caracterización formal de los tratamientos

Dudas y aclaraciones



Muchas gracias!

Xabier Arrieta

Joseba Enjuto

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