Gobierno de Navarra

Plan de Seguridad Corporativo del Gobierno de Navarra

Tudela, 21 de marzo de 2007

Plan Director de Seguridad del Gobierno de Navarra

Índice

Plan Director de Seguridad del Gobierno de Navarra

Índice

Protección de datos de carácter personal

Según el profesor Davara:

"La protección de los datos de carácter personal es el amparo debido a los ciudadan
contra la posible utilización por terceros, en forma no autorizada, de sus dat
personales para, de esta forma, confeccionar una información que, identificable c
él, afecte a su entorno personal, social o profesional, en los límites de su intimidad

La principal legislación española en la materia es:

- La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carác personal (LOPD)
- El Real Decreto 994/1999, de 11 de junio, por el que se desarrolla el Reglamento Medidas de Seguridad de los ficheros automatizados que contengan datos carácter personal (RMS)

Aspectos generales de la LOPD

- Se aplica a los ficheros (automatizados o no) que contengan datos de carácter personal
- Se rige por el principio de calidad de los datos, que significa que los datos objeto de tratamiento deben:
  - recabarse para una finalidad o finalidades determinadas, expresas y legítimas
  - ser pertinentes, adecuados y no excesivos para la finalidad para la que se han recabado recogido
  - mantenerse exactos y puestos al día
  - no pueden permanecer en el fichero más tiempo del que resulte necesario para la finalida para la que se recabaron
- Exige, en principio, el consentimiento del afectado
- Hay que informar al afectado en la recogida de datos
- Se deben adoptar todas las medidas necesarias para garantizar la seguridad de los datos personales

Datos especialmente protegidos

- **Protección máxima:** ideología, afiliación sindical, religión o creencias
- **Protección alta:** origen racial, salud o vida sexual
- **Prohibición** de crear o mantener ficheros con la finalidad exclusiva almacenar datos que revelen ideología, afiliación sindical, religió creencias, origen racial o étnico y vida sexual
- Los datos relativos a la **comisión de infracciones penales administrativas** sólo podrán ser incluidos en ficheros de l Administraciones Públicas competentes en los supuestos previstos en l respectivas normas reguladoras

Ficheros de titularidad pública

- La creación, modificación y supresión de ficheros de titularidad pública de hacerse por medio de disposición general publicada en el BOE o Boletín Oficial de Comunidad Autónoma correspondiente.
  - En el Gobierno de Navarra, en virtud del Decreto Foral 143/1994, de 26 de jul por el que se regulan los ficheros informatizados con datos de carác personal, dependientes de los órganos de la Administración de la Comunid Foral de Navarra y de sus Organismos Autónomos, mediante Orden Foral Consejero del departamento al que pertenece la unidad responsable del fiche
- Es obligatoria la inscripción del fichero en el Registro de Protección de Datos de Agencia Española de Protección de Datos
- Debe existir un procedimiento para que el afectado pueda ejercitar los derechos impugnación, acceso, rectificación y cancelación.

Situación en Gobierno de Navarra en Septiembre de 200

- Conocimiento relativo, entre los responsables, de las exigencias de la LOPD y demás legislación aplicable.
- No se informaba al afectado de la existencia de un fichero con datos de carácter personal
- Inexistencia de procedimiento y normativa que obligase a hacer cumplir la LOPD a los responsables de los ficheros.
- Existencia de ficheros con datos de carácter personal sin declarar a la AEPD.
- Problemas con los cambios de estructura, pues cambian las unidades responsable y las unidades ante las que el afectado puede ejercer sus derechos, y no se hace traslado de ello a la AEPD.
- Inexistencia de cláusulas de confidencialidad en los contratos de los empleados.
- En los contratos de externalización de servicios no se contemplaban las cláusulas que exige la normativa.

Reglamento de Medidas de Seguridad (RMS)

Características

- Es de aplicación a los ficheros automatizados que contengan datos de carácter personal
- Establece los niveles de seguridad que, según el tipo de datos, debe tener asignado ca fichero o tratamiento
- Establece la obligación de **adoptar medidas técnicas y organizativas** que prevengan la
  - alteración
  - pérdida
  - tratamiento o acceso no autorizado

  de los datos de carácter personal
- Obliga a la existencia de un Documento de Seguridad en el que se recojan todas las medic técnicas y organizativas, así como las funciones y obligaciones de las personas que acceden los datos
- Está por desarrollar el reglamento para los ficheros no automatizados, aunque ya circula ciertos ámbitos el nuevo Reglamento de medidas de seguridad que, entre otras cosas, ya contemplaría

Características

veles de seguridad

Ficheros que contengan algunos de los siguientes tipos de datos, cuando no constituyan un perfil

- Identificativos
- Características personales
- Circunstancias sociales
- Académicos y profesionales
- Empleo y carrera administrativa
- Información comercial
- Económico-financieros
- Transacciones

NIVEL BÁSICO

Ficheros que contengan datos:

- Del nivel Básico, que permitan obtener un perfil de la persona
- Sobre infracciones penales y administrativas
- De Hacienda Pública
- De servicios financieros
- De solvencia patrimonial y crédito

(Es obligatorio auditarlos cada 2 años)

NIVEL MEDIO

Ficheros que contengan datos

- Especialmente protegidos (ideología, creencias, religión, origen racial, salud o vida sexual)
- Recabados para fines policiales

(Es obligatorio auditarlos cada 2 años)

NIVEL ALTO

Características

pos de medidas

TÉCNICAS	ORGANIZATIVAS
Control de acceso lógico	Documento de seguridad
Identificación y autenticación	Funciones y obligaciones del personal
Notificación y gestión de incidencias	Responsable de seguridad
Gestión de soportes	Notificación y gestión de incidencias
Copias de respaldo y recuperación	Control de acceso físico
Telecomunicaciones	Distribución de soportes
Auditoría	Auditoría

Objetivos

Objetivos del RMS en la recogida de datos

- Analizar la naturaleza (el tipo) de datos que se recogen
- Identificar el origen de los datos y la finalidad para la que se van a utilizar

  En función de estos dos puntos, se determina el nivel de seguridad que se tiene que aplicar: básico, medio o alto
- Poder hacer una correcta declaración del fichero a la AEPD
- Determinar el grado de cobertura legal para el manejo de los datos captados
- Verificar que el titular de los datos tiene o puede recibir información sobre sus derechos con respecto a los datos recogidos y que existe un circuito establecido para atender las peticiones sobre información, rectificación y cancelación

Objetivos

bjetivos del RMS en el proceso y/o almacenamiento de la información: QUE

La seguridad de los sistemas de información se rija por unas políticas, normas y procedimient
ecuados

Exista una arquitectura de seguridad y esté supervisada por un(os) Responsable(s) de Segurida

Exista una aprobación formal por la Dirección de las políticas y de la figura del Responsable
eguridad

Haya conocimiento por parte del personal de las políticas de seguridad y de las repercusion
e puede acarrear su incumplimiento.

Exista un registro de incidencias

Existan medidas de control sobre el acceso físico a las instalaciones

Existan medidas de control sobre el acceso lógico a la información

Existan medidas de control en el entorno de desarrollo para el manejo de datos de prueba y pa
control de pases a producción

Para los casos en los que todo o parte de los servicios estén soportados por empresas extern
utsourcing) determinar el grado de cobertura legal (contractual) existente con el proveedor
rvicio en lo que respecta a los estados de la seguridad

Objetivos

bjetivos del RMS en la salida de información

- Garantizar el derecho a la intimidad del titular de los datos
- Garantizar el control sobre los soportes magnéticos que salen de la instalación
- Garantizar el control sobre la posibilidad de bajar información sensible desde e torno de producción a soporte magnético o de cualquier otro tipo
- Garantizar la protección contra el envío de información sensible fuera de la stalación a través de otros canales (e-mail u otros)
- Garantizar la calidad de la información de salida, su consistencia e integridad
- Determinar el grado de cobertura legal para la cesión de datos o el uso de datos didos

Situación en Gobierno de Navarra en Septiembre de 2003

- No existía el “Documento de Seguridad” del Gobierno de Navarra
- Sólo unas pocas aplicaciones disponían de Documento de Seguridad y, en este aso, no estaba actualizado
- Inexistencia de las medidas técnicas y organizativas recogidas en el RMS
- No se tenía el rigor requerido en las auditorías preceptivas. Sólo se realizó una de la ase de Datos de Contribuyentes en el año 2001
- Caso de que existiesen los logs, no cumplían con los requisitos a que obliga el RMS
- Las personas desconocían sus funciones y obligaciones en el tratamiento de la formación
- La información no estaba clasificada y tampoco existían guías de clasificación
- No se impartía ningún tipo de formación en seguridad y protección de datos

Plan de Seguridad Corporativo

Problemática

Legislación

Plan de Modernización

Plan Sociedad Información

NECESIDAD DE ACOMETER UN PLAN ESTRATÉGICO DE SEGURIDAD CORPORATIVO

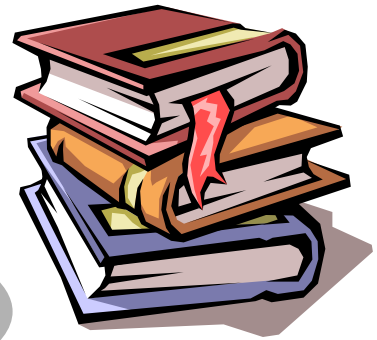
Plan de Seguridad Corporativo

- **Concretamente:**
  - Para aportar confianza al despliegue del Plan de Modernización de la Administración y del Plan de la Sociedad de la Información.
  - Para alinear la seguridad a las necesidades de la actividad, los sistemas y la tecnología del Gobierno de Navarra y definir el nivel objetivo de seguridad
  - Para cumplir con la legislación vigente (LOPD, LSSI, Firma electrónica, Ley 30/1992...)
  - Para definir el Plan de Acción con el fin de obtener el nivel objetivo de seguri
  - Para cuantificar las inversiones y gastos para conseguir el nivel objetivo de seguridad
  - Para definir un plan de concienciación de las personas en los temas de seguridad
  - Para aportar confianza en el uso de las tecnologías de la información

Plan de Seguridad Corporativo

El Gobierno de Navarra acordó aprobar, el 17 de mayo de 2004, **El P**
de Seguridad de la Información y las Comunicaciones del Gobier
de Navarra, que constituye el marco de referencia que define la estrate
y gestión de la seguridad de la información en los aspectos organizativ
normativos, tecnológicos y de procedimiento, y que está compuesto
dos documentos:

- **Política de Seguridad**
- **Catálogo de Proyectos y productos finales**



Protección de datos

Objetivos

- Definir un **Modelo de Seguridad Corporativo** alineado con el Plan de Moderniza existente, es decir, se ha definido el *nivel de seguridad objetivo* del Gobierno de Nava
- Identificar el **nivel de seguridad** existente en ese momento en los sistemas información del Gobierno de Navarra.
- Definir y planificar el **conjunto de acciones a realizar** (a corto, medio y largo plaz raíz de la diferencia existente entre el nivel de seguridad objetivo del Gobierno Navarra y del nivel de seguridad en ese momento.
- Planificar las **inversiones y costes necesarios** para alcanzar el nivel de segur adecuado a las necesidades de negocio del Gobierno de Navarra.

Implantación del Plan de Seguridad Corporativo

- Los proyectos se abordan inicialmente **por Departamentos o áreas**.
- Se utilizan **enfoques metodológicos** en los proyectos que permitan **extensión** a otras áreas del Gobierno.
- Que los **resultados** obtenidos sean fácilmente **reutilizables.**

- Cada proyecto se compone de las siguientes fases:
  - Realización de un **diagnóstico detallado** de la situación actual.
  - Definición de un **plan de acción.**
  - Identificación y evaluación de los **recursos y herramientas** necesarias para la implantación
  - **Implantación.**

Implantación del Plan de Seguridad Corporativo

- Los proyectos que **se decide abordar** en la primera parte de la implantación son los siguientes:
  - **Adaptación a la LOPD y al Reglamento de Medidas de Seguridad que le acompaña**
  - **Posicionamiento respecto a la norma ISO 17799 en su versión de 2005**
  - Desarrollo de las guías para el inventario y la clasificación de activos tecnológicos
  - Realización del inventario de activos
  - **Diseño de un modelo de autorizaciones de acceso a aplicaciones basado en roles**
  - Desarrollo de una metodología de Análisis y Gestión de Riesgos Tecnológicos
  - Diseño de un modelo de gestión segura de soportes
  - Desarrollo de una metodología para contemplar la Seguridad en el Ciclo de Vida del Desarrollo de Servicios
  - Protección de datos reales en entorno de prueba
  - Revisión del actuales procesos de gestión de contenidos en servidores públicos
  - Integridad de contenidos en servidores públicos

Implantación del Plan de Seguridad Corporativo

- Los Departamentos o unidades en las que **se han abordado** algunos de los proyectos enmarcados en el Plan de Seguridad Corporativo fueron:

  - Organismo autónomo **Hacienda Tributaria de Navarra**
  - Departamento de **Agricultura, Ganadería y Alimentación**
  - Organismo autónomo **Estación de Viticultura y Enología de Navarra**
  - Departamento de **Industria y Tecnología, Comercio y Trabajo**
  - Organismo autónomo **Servicio Navarro de Empleo**
  - Dirección General de **Justicia**
  - Organismo autónomo **Instituto Navarro de Bienestar Social**

Complejidad de la aplicación de la LOPD y el RMS

- **Estructura orgánica cambiante**: varían las unidades responsables ante las que afectado puede ejercer sus derechos.
- **Diversidad de responsables**: **desconocimiento de las exigencias de la LOPD** demás legislación aplicable.
- Dificultad para implantar en una Administración las **medidas organizativas de l que habla el RMS.**
- Gran incremento de la **externalización de servicios.**
- Necesidad de mantener **almacenes de información** para que las **políti públicas** sean cada vez más **eficientes**.
- Necesidad de otros Departamentos de **conocer información** residente en fiche de los **que no son titulares**.
- Dificultad para **clasificar la información** administrativa, dado su **volumen variedad**.

Conclusiones

Mejora de **seguridad en marcha.**

Nuevas funciones y responsabilidades relacionadas con la organización de la seguridad que es necesario asignar.

Necesidad de dotar de **instrumentos eficaces** para la realización de las funciones de seguridad.

La **situación** en todos los Departamentos analizados es muy **similar.**

Extensión vertical poco efectiva, ya que los planes de acción departamentales son similares.

NUEVO IMPULSO

Estrategia futura

NUEVO IMPULSO

an de Seguridad Corporativo

Navarra Digital Segu

Estrategia futura

n de Seguridad
Corporativo

- **Consolidación** de los resultados obtenidos.
- **Orden Foral sobre Normas de Uso de los Sistemas Información y las Comunicaciones en la Administración de la Comunidad Foral de Navarra.**
- Extensión al resto de departamentos del Gobierno de Navarra de los proyectos realizados (**extensión horizontal**)
- Ir a **soluciones corporativas** de rápida implantación e todos los departamentos.
- Creación de **Espacio de Seguridad**, como instrument para realizar las funciones de seguridad.

Estrategia futura

Navarra Digital Segura

"Potenciar el Desarrollo Regional de Navarra e torno al área de la Seguridad de la Información las Comunicaciones, haciendo de Navarra un Comunidad referencial a nivel mundial e tecnologías y servicios avanzados de seguridad"

Fin de la presentación

Gobierno de Navarra