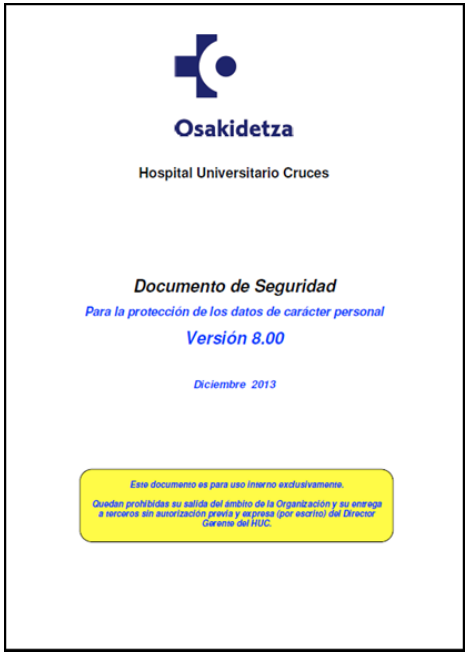
Automatización de los controles de seguridad

Begoña Carranza
Hospital Universitario Cruces

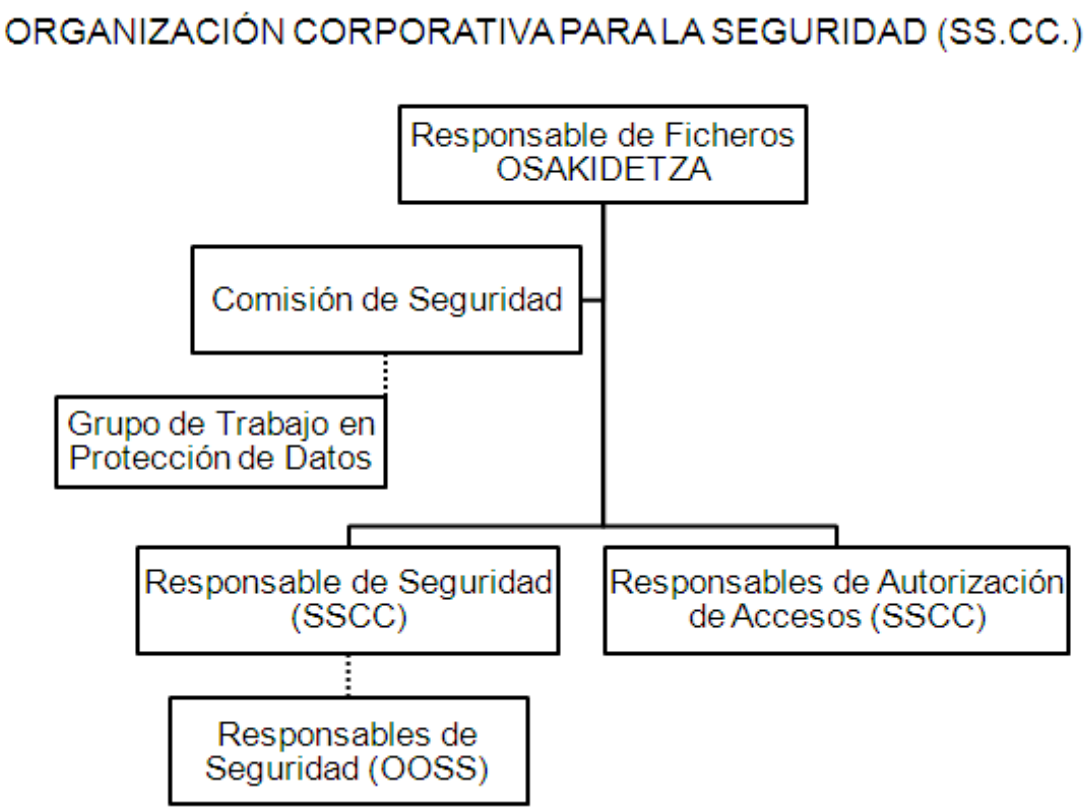
Antecedentes

- L.O.15/1999. LOPD
- R.D. 1720/2007. RLOPD

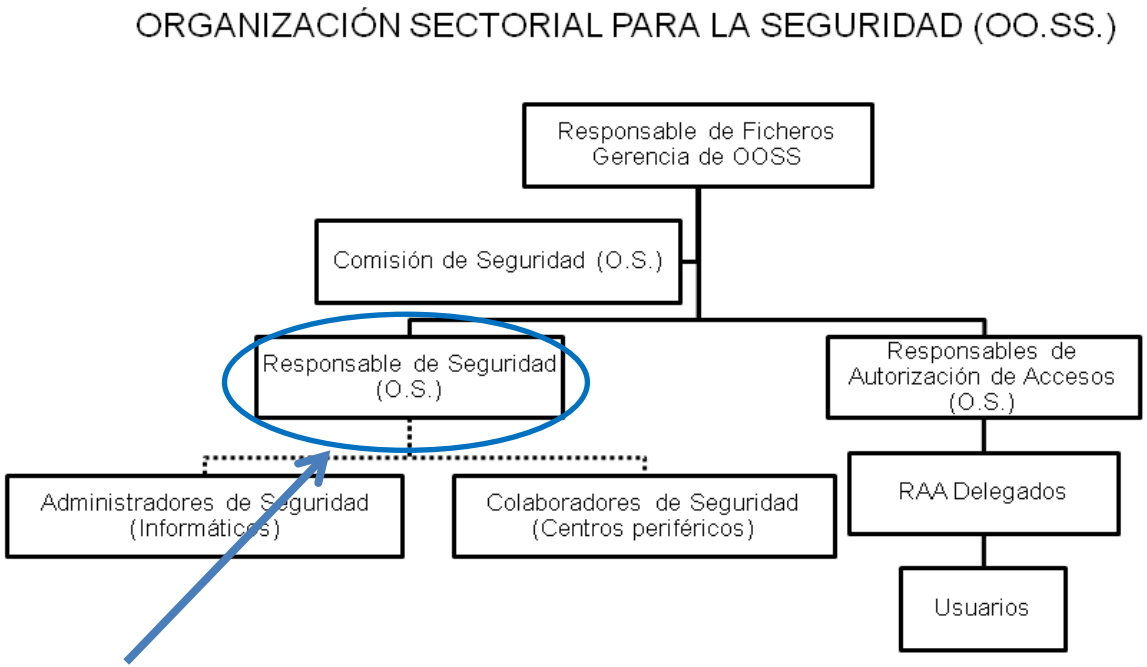


Medio/Alto

Organización de Seguridad en Osakidetza



Organización de Seguridad en HUC



Realiza controles seguridad

¿Cómo?

Control semanal

- Usuarios sospechosos:
  - No se ajustan al modelo corporativo (DNI)
  - Tienen privilegios de administrador

- Usuarios que han superado el período de cambio obligatorio de contraseña → BAJA

INFORME SEMANAL (09/09/2015):
CONTROLES PERIÓDICOS DE LOS ACCESOS A LAS APLICACIONES ASISTENCIALES

SERVICIO DE
HOSPITAL UN

CONTROL DE CUENTAS DE USUARIO DE APLICACIONES OSAKIDETZA

1) SE HA DADO DE BAJA A LOS SIGUIENTES USUARIOS NO PROVISIONALES PORQUE SU CUENTA ESTÁ CADUCADA (EXPIRADA) EN EL DIRECTORIO ACTIVO:

USUARIO	NOMBRE	FECHAPAS	OBSERVACIONES
[redacted]	[redacted]	9/1/2014	Cuenta EXPIRADA en el Directorio Activo el 02/09/2015 7:00:00
[redacted]	[redacted]	5/6/2014	Cuenta EXPIRADA en el Directorio Activo el 02/09/2015 7:00:00
[redacted]	[redacted]	2/6/2015	Cuenta EXPIRADA en el Directorio Activo el 02/09/2015 7:00:00
[redacted]	[redacted]	17/6/2013	Cuenta EXPIRADA en el Directorio Activo el 02/09/2015 7:00:00
[redacted]	[redacted]	27/1/2014	Cuenta EXPIRADA en el Directorio Activo el 02/09/2015 7:00:00
[redacted]	[redacted]	13/7/2015	Cuenta EXPIRADA en el Directorio Activo el 02/09/2015 7:00:00

2) SE HA DADO DE BAJA A LOS SIGUIENTES USUARIOS NO PROVISIONALES POR LLEVAR MÁS DE 45 DÍAS SIN HACER EL CAMBIO OBLIGATORIO DE PASSWORD (EXIGIDO CADA 120 DÍAS):

USUARIO	NOMBRE	FECHAPAS	OBSERVACIONES
[redacted]	[redacted]	21/3/2015	El usuario **pertenece** al HOSPITAL DE CRUCES y está **habilitado** en el Directorio Activo.
[redacted]	[redacted]	25/3/2015	El usuario **pertenece** al HOSPITAL DE CRUCES pero está **deshabilitado** en el Directorio Activo.
[redacted]	[redacted]	25/3/2015	El usuario **pertenece** al HOSPITAL DE CRUCES y está **habilitado** en el Directorio Activo.
[redacted]	[redacted]	27/3/2015	El usuario **pertenece** al HOSPITAL DE CRUCES y está **habilitado** en el Directorio Activo.

3) Nº DE USUARIOS NO PROVISIONALES ACTIVOS: 2697

4) SE HA DADO DE BAJA A LOS SIGUIENTES USUARIOS PROVISIONALES POR HABER SIDO ASIGNADOS HACE MÁS DE 6 DÍAS:

USUARIO	NOMBRE	FECHAPAS
NINGUNO		

5) USUARIOS SOSPECHOSOS (=RAROS) ACTIVOS:

USUARIO	NOMBRE	FECHAPAS
NINGUNO		

6) USUARIOS CON PRIVILEGIOS SOSPECHOSOS ACTIVOS (1: SUPERVISOR, 2: ADMINISTRADOR APLICACIÓN):

USUARIO	NOMBRE	TIPONIVEL	FECHAPAS
NINGUNO			

Control mensual

- Control estadístico de accesos a las aplicaciones
- Intentos de acceso indebidos
- Software comercial: facilitar acceso a los datos de logging

INFORME MENSUAL (01/7/2015 00:00:00 - 31/07/2015 23:59:59)
ACCESOS A LAS APLICACIONES

ACCESOS REGISTRADOS A LAS APLICACIONES

APLICACIÓN	ACCESOS
Solicitud Citas	5269
Rii	762
Sol. Incorporación tecnológica	260
DIETOOLS - Gestión usuarios	148
Registro	131
Recuperar mis contraseñas	122
Memoria	115
Medulares	88
Admin de Usuarios y Aplicaciones	87
Retén Celadores	61
Rx Informados	54
interconsultas	43
ACTAS	43
Admin de Responsables de Carpetas	29
Sesiones Clínicas	26
Portal del Residente	13
Adquisición equipos	8
Consultas LDAP	5
Plan de Conting. Órdenes Médicas	3
Conferencias Clínicas	2
Divulgaciones	2
Encuestas de Formación	1
Gestión de Residentes	1
Gestión de camas	1
CMI - Publicación de Informes	1

POSIBLES INTENTOS DE ACCESO INDEBIDO REGISTRADOS

DÍA	ACCESO	CANTIDAD
01/07/2015 (Miércoles)	AWC	8
02/07/2015 (Jueves)	AWC	32
02/07/2015 (Jueves)	Rii	3
03/07/2015 (Viernes)	AWC	31
03/07/2015 (Viernes)	Rii	1
04/07/2015 (Sábado)	AWC	2
06/07/2015 (Lunes)	AWC	13
06/07/2015 (Lunes)	Rii	1
07/07/2015 (Martes)	AWC	24
07/07/2015 (Martes)	Rii	4
08/07/2015 (Miércoles)	AWC	11
09/07/2015 (Jueves)	AWC	11

Control trimestral

- BD →Recursos compartidos – responsable de cada recurso
- Comunicación a los responsables sobre las personas autorizadas al recurso y el tipo de acceso
- Respuesta positiva

Osakidetza

SERVICIO DE INFORMÁTICA
HOSPITAL UNIVERSITARIO CRUCES

Controles LOPD Hospital Universitario Cruces
31/03/2015

Esta comunicación pretende garantizar ***el cumplimiento de las obligaciones legales y reglamentarias establecidas en el Reglamento de Desarrollo de la LOPD (RLOPD)***. En concreto, dicho Reglamento establece la obligación de realizar controles periódicos, además de otras medidas de seguridad catalogables, en sí mismas, como "***controles de seguridad***".

La L.O. 15/1999 (LOPD) establece en su artículo 44.3.h, como infracción de carácter grave, "mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

El Documento de Seguridad del Hospital Universitario Cruces dispone en su norma 70, relativa a la "Regulación de los controles periódicos a realizar para la verificación de lo dispuesto en el documento de seguridad", lo siguiente:

B. TRIMESTRALMENTE:

4) Se debe revisar el contenido de los siguientes registros:

- ***Inventario de usuarios con acceso autorizado a datos de carácter personal (tratamiento automatizado y no automatizado).***

Con objeto de implantar las medidas de seguridad establecidas en el RLOPD y llevar a cabo todos los controles periódicos, normas y procedimientos contemplados en el Documento de Seguridad de este Hospital sobre las carpetas que tratan y albergan datos de carácter personal, **periódicamente le enviaremos información de las carpetas en "S" solicitadas por su Servicio**, así como la **relación de las personas** que tienen acceso a las mismas y que cuentan con su autorización.

Si detecta cualquier anomalía en la lista de personas autorizadas, le rogamos se ponga en contacto con el Servicio de Informática a través de la aplicación Rii pinche aquí para acceder

Begoña Carranza
Responsable de Seguridad

Usuarios autorizados sobre la carpeta S:\DS-Cruces

[redacted]	SUBDTOR/A GESTION DE HOSPITAL G1	Leer
[redacted]	DIRECTOR/A MEDICO HOSPITAL G1	Leer
[redacted]	J. DE SERVICIO SANITARIO	Leer
[redacted]	SUBDIRECTOR/A MEDICO HOSPITAL G1	Leer
[redacted]	J. DE SERVICIO ADMON. Y GESTION	Leer
[redacted]	SUBDTOR/A GESTION DE HOSPITAL G1	Leer
[redacted]	TCO SUPERIOR ADMON. Y GESTION	Leer
[redacted]	DIRECTOR/A PERSONAL HG1	Leer
[redacted]	DIRECTOR/A ECONOM.-FINAN. HOSP. G1	Leer
[redacted]	DIRECTOR/A GERENTE HOSPITAL G1	Leer
[redacted]	J. DE SERVICIO SANITARIO	Leer

Otras iniciativas

- Logging mediante TPE en aplicaciones propias
- Uso de https, comunicaciones cifradas, con certificados…
- Exigir a los proveedores información para el control de la seguridad
- Cuadro de mando de seguridad