

Protección de los Datos Personales de la historia clínica en Argentina y Uruguay e IHE XDS

Resumen—En 2000, Argentina, gracias a su ley sobre protección de datos personales (PDP)¹, ha sido el primer país suramericano considerado país seguro por la Unión Europea y la Agencia Española de Protección de Datos (AEPD). Uruguay siguió el mismo camino en 2008². Concomitantemente, ambos países publicaron también una ley definiendo los “Derechos del Paciente”, que contienen artículos relativos a su historia clínica³. Presente en forma muy similar en todos estos textos, el “consentimiento” es el filtro que define el grado de confidencialidad de los varios documentos de la historia clínica de un paciente. Este consentimiento puede ser complejo, es revocable, transitivo y requiere para su aplicación la preexistencia de un “Sistema de Gestión de Seguridad de la Información” (SGSI). Explicaremos la referencia implícita de ambas leyes de PDP a la familia de estándares ISO/IEC 27000, para la instalación y mejora continua del SGSI, que asegura confidencialidad a priori, disponibilidad de los datos, integridad de los documentos, imputabilidad (“accountability”) de los profesionales y auditabilidad de las transacciones. En la segunda parte del artículo, demostraremos que los requisitos del SGSI y del “consentimiento” están cumplidos por la arquitectura “Cross-Enterprise Document Sharing” (XDS) basada en la orquestación de transacciones entre actores implementados acorde a perfiles de integración definidos por “Integrating the Healthcare Enterprise” (IHE).

Abstract—In 2000, Argentina, in virtue of its law on the protection of personal data (PDP), became the first latin american country considered “safe” by the european union and Spanish Agency for Data Protection (AEPD). Uruguay followed the same path in 2008. Meanwhile, both countries also published a law on the “Patient Rights”, containing articles about her/his clinical history.

In all of these texts, the “consent” is the filter which defines the level of confidentiality of the various documents of a patient healthcare history. This consent may be complex, is revocable, transitive and requires the preexistence of an “Information Security Management System” (ISMS). We shall make explicit the implicit reference of both PDP laws to ISO/IEC 27000 family of standards for the installation and continued improvement of the ISMS, which warranties a priori confidentiality, availability of data, integrity of documents, accountability of professionals and auditability of the transactions.

In the second part of the article, we shall demonstrate that all the requirements of the ISMS and of the “consent” are fulfilled by the architecture “Cross-Enterprise Document Sharing” (XDS) based on the orchestration of transactions between actors modeled according to integration profiles defined by “Integrating the Healthcare Enterprise” (IHE).

Temas claves—Datos personales, Derecho del paciente, Historia clínica, Consentimiento informado previo, Sistema de Gestión de la seguridad de la información, SGSI, ISO/IEC 27000, ISO/IEC 27002, ISO/IEC 27799, IHE, XDS, BPPC.

I. NOMENCLATURA

AEPD	Agencia Española de Protección de Datos
AR	Argentina
ATNA	Audit Trail and Node Authentication
BPPC	Basic Patient Privacy Consent

IHE	Integrating the Healthcare Enterprise
ISMS	(SGSI) Information Security Management System
PIX	Patient Index
PDP	Protección de Datos Personales
PDQ	Patient Demographic Query
SGSI	(ISMS) Sistema de Gestión de la seguridad de la Información
UY	Uruguay
XDS	Cross-Enterprise Document Sharing
XUA	Cross-Enterprise User Authentication

II. INTRODUCCIÓN

Tanto la legislación Argentina como la Uruguaya, en materia de protección de datos personales (PDP) e historia clínica, son similares en cuanto a obligaciones y derechos. En ambos casos el consentimiento es la columna vertebral.

Categorías de datos

Los identificadores (Nombre, Apellido, Fecha de Nacimiento, Cédula, nacionalidad, domicilio, fecha de nacimiento y otros datos de fuente pública) no requieren consentimiento para su recolección y uso. Cualquier otro dato personales y dato personal sensible (encontrándose la historia clínica dentro de esta última categoría⁴) requiere consentimiento. Ambas legislaciones expresan la no obligatoriedad de suministrar datos sensibles⁵, y autorizan como excepción, entre otras, al tratamiento de estos con fines estadísticos o científicos cuando no puedan ser identificados sus titulares (disociación de datos)⁶ y a los servicios y profesionales de la salud de salud⁷.

Consentimiento

Se entiende como la autorización que otorga una persona para que sus datos personales sean utilizados. En ambos Argentina y Uruguay, para la recolección de datos se debe contar con el “consentimiento libre, expreso, previo e informado” del titular de los datos. Son excepciones a esto la recolección que derive de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento⁸. Por lo cual, cuando un paciente visita su médico, toda la información de salud recabada por el médico no requiere consentimiento para entrar en la historia clínica.

No obstante, resulta frecuente en la práctica médica la necesidad de suministrar datos a terceros, sea por fines administrativos o del tratamiento. Las leyes de PDP a que nos referimos contemplan la cesión o comunicación de datos con y sin consentimiento de la siguiente forma⁹:

“- Los datos personales sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

- El consentimiento para la cesión es revocable.
- A su vez obligan al cesionario a cumplir con las mismas obligaciones legales del cedente el cual responderá solidariamente ante los organismos de control.
- El consentimiento no es exigido cuando se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados."

En caso de transferir la historia clínica a otros países, las legislaciones argentina y uruguaya¹⁰:

"- prohíben la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados y

- permiten la transferencia internacional de datos tratándose de intercambio de datos de carácter médico, cuando lo exija el tratamiento del afectado. Tratándose de una investigación epidemiológica los datos deberán estar disociados, es decir separados de su contenido patronímico."

Seguridad de la información

Para la aplicación de todas estas reglas de confidencialidad, *"se deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado"*¹¹.

Luego hacen mención a los registros de acceso y la auditabilidad cuando dicen que las medidas de seguridad deben permitir *"detectar desviaciones, intencionales o no, de información"* independientemente que los riesgos provengan de *"la acción humana o del medio técnico utilizado"*.

Referencia implícita a ISO 27000

Todo hace pensar que el modelo de seguridad y confidencialidad implícito de las PDP argentina y uruguaya son la familia de estándares ISO/IEC 27000: Existen institutos de estandarización y normalización que promueven y capacitan en la familia de normas ISO/IEC 27000 entre otras (AR: IRAM, UY: UNIT). La Dirección Nacional de Protección de Datos Personales en Argentina integra un representante del IRAM en su Consejo Consultivo. Organismos como el ONTI y ArCERT¹² (dependientes de la Secretaría de la Gestión Pública Rep. Argentina) adoptaron para la administración nacional la norma ISO/IEC/IRAM 17.799 (que se transformó en 27002 en 2005). La AGESIC, unidad de regulación de la PDP en el Uruguay, publicó "Buenas Prácticas en Seguridad de la Información"¹³, donde se refiere explícitamente al uso de las normas UNIT/ISO/IEC 27000 para establecer el SGSI.

Introducción a ISO/IEC 27000

Pues no podemos pasar por alto las ISO/IEC 27000. Para organizar un SGSI en el sector salud son importantes: ISO/IEC 27001:2005, Requisitos de SGSI; ISO/IEC 27002:2005, Código de Prácticas para GSI; ISO/IEC 27799:2008, Guías para SGSI en el sector de la Salud.

Estos estándares explican como establecer, Implementar, Operar, Monitorear, Revisar, Mantener y Mejorar un SGSI. Tal sistema incluye el aspecto informático pero también todo el entorno, inclusive el factor humano. Corresponde con las atribuciones del responsable de bases de datos en las leyes de PDP mencionadas. que dicen que el responsable de las bases de datos deberá garantizar las medidas técnicas y organizativas que resulten idóneas para garantizar integridad, confidencialidad y disponibilidad.

ISO/IEC 27799: Gestión de la seguridad específica de la Información en salud, utilizando ISO/IEC 27002

El sector salud, como los otros sectores de actividad, puede instalar un SGSI utilizando ISO/IEC 27002. Es lo que hicieron Australia, Canadá, Francia, Países Bajos, Nueva Zelanda, Africa del Sur. Luego de analizar estas experiencias, ISO/IEC publicó ISO/IEC 27799, que complementa ISO/IEC 27002 y precisa particularidades del sector salud que requieren especialización de los principios organizativos y controles. Entre otros:

Confidencialidad/Disponibilidad

Los PDP clasifican la historia clínica como "dato sensible especialmente protegido". ISO/IEC 27799 agrega : "las organizaciones sanitarias deberán clasificar uniformemente la información personal como confidencial"¹⁴ con los argumentos siguientes: la confidencialidad de la información personal de salud suele ser en gran medida subjetiva, en lugar de objetiva; la confidencialidad de la información personal de salud depende del contexto; la confidencialidad de la información personal de salud puede cambiar durante la vida útil de registro de salud de un individuo;

Identificación correcta del paciente

Los sistemas de información utilizados para el procesamiento de la información personal de salud deberá: asegurarse de que cada paciente pueden ser identificados de forma unívoca dentro del sistema; ser capaces de combinar los registros duplicados o múltiples, si se determina que los registros múltiples para el misma tema de la atención han sido creados de forma involuntaria o durante una emergencia médica¹⁵.

Disociación

Los procedimientos utilizados para el procesamiento de la información personal de salud debe garantizar que los datos de identificación personal que han sido derivados solo se mantienen cuando es necesario, que la supresión, las técnicas disociación y generación de seudónimos son utilizadas de manera apropiada para reducir al mínimo el riesgo de revelación o fuga no intencional de la información personal¹⁶.

Integridad de los documentos, imputabilidad de las personas y auditabilidad de las transacciones

corresponden a la responsabilidad personal de los empleados de instituciones médicas y a la fiscalización de la misma. Implica un sistema de archivado con enmienda por edición de nuevo documento en lugar de modificación aplicada dentro del documento mismo, y por otro lado implica también la existencia de una bitácora automática exhaustiva de todas las transacciones con documentos¹⁷.

Introducción a IHE XDS

ISO/IEC 27000 es agnóstico en cuanto a las tecnologías usadas para aplicar sus principios de organización. En este trabajo, damos un paso más, con nuestra hipótesis que el modelo de integración Integrating the Healthcare Enterprise (IHE) Cross-Enterprise Document Sharing (XDS) propone una solución tecnológica completa para realizar los principios de organización de ISO/IEC 27002, ISO/IEC 27779, y PDP Argentina y Uruguay.

IHE describe flujos reales de la información dentro del hospital y formas de estandarizarlos con orquestación de transacciones de transmisión de documentos entre actores.

El tipo fundamental de documento a almacenar, transportar y consultar en una orquestación XDS es el Documento Clínico (CDA release 2). Este formato estructura cualquier nuevo evento de la historia clínica (consulta, resultados de laboratorios, informe médico, corrección de informe médico, ...). El CDA se usa también como estructura de documentos particulares como por ejemplo: el documento imagenológico (XDS-I), el documento escaneado (XDS-SD), y de primordial importancia para PDP, el documento Basic Patient Privacy Consent (BPPC).

III. METODOLOGÍA

(A) Definir los 4 grupos de datos funcionalmente necesarios para instalar PDP en la historia clínica: (a) Consentimientos, (b) Datos patronímicos, (c) Datos comunes y sensibles que necesitan consentimiento antes registrarse, (d) Datos de bitácora de transacciones relativas a los datos necesitando consentimiento.

(B) Encontrar los actores IHE correspondientes con los grupos de datos personales.

(C) Estudiar la flexibilidad de BPPC para registrar los consentimientos informados previos

(D) Plantear varios casos de acceso: (4) por paciente, familiar, médico o administrativo de la institución, (5) por médico de otra institución, (6) para trabajo científico; y averiguar si IHE XDS permite aplicar los principios definidos en ISO 27000 en cada uno de estos casos.

IV. DESARROLLO

(A) 4 categorías de datos necesarios para una historia clínica aplicando PDP

(a) Los consentimientos informados previos permiten definir la confidencialidad de la información para cada paciente en forma subjetiva, con cualquier grado de especificidad. Por ejemplo, el paciente puede aceptar de compartir datos de salud sexual con los cardiólogos, pero no con los dentistas, o más complejo aún, la ley uruguaya reconoce al paciente el "derecho a no saber"¹⁸: *“En situaciones excepcionales y con el único objetivo del interés del paciente con consentimiento de los familiares se podrá establecer restricciones al derecho de conocer el curso de la enfermedad o cuando el paciente lo haya expresado*

previamente (derecho a no saber).Este derecho a no saber puede ser relevado cuando, a juicio del médico, la falta de conocimiento pueda constituir un riesgo para la persona o la sociedad.”

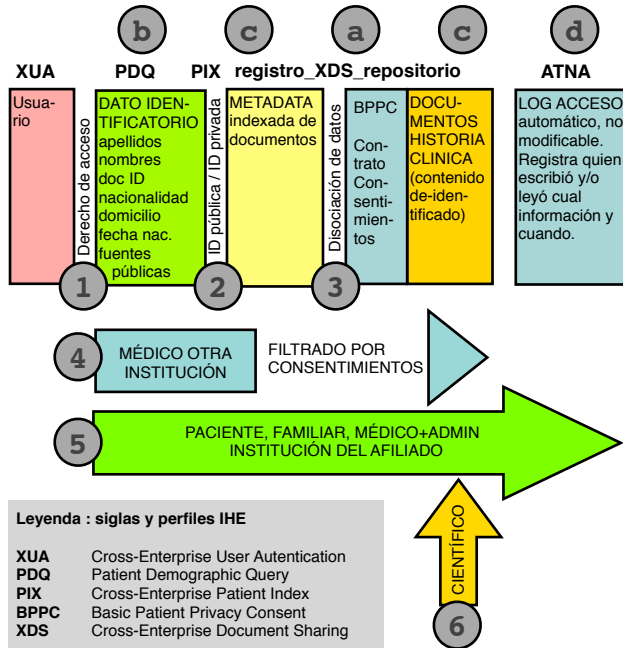
Pues el acceso a la información de salud en sí depende necesariamente de un sistema muy flexible de gestión de consentimientos informados definiendo la privacidad de la información. A su vez, tal sistema debe filtrar, pero sin frenar la información autorizada en razón del carácter eventualmente crítico de la disponibilidad de la información, por ejemplo cuando se requiere información a la ocasión de emergencias médicas. Como consecuencia, una política de permisos de acceso automatizada parece imprescindible y constituye un desafío mayor para sistemas informáticos de salud.

(b) Los datos identificatorios son libres de consentimiento previo tanto en la ley argentina que la ley uruguaya. Eso permite usarlos como clave para acceder a los documentos de consentimiento del paciente, antes proceder eventualmente a la búsqueda de los documentos substanciales autorizados de la historia clínica de dicho paciente.

(c) Juntamos en una sola categoría los datos que necesitan consentimiento antes registrarse o consultarse. No los subdividimos en varias categorías, separando por ejemplo la categoría de los datos sensibles, porque en el Uruguay, la ley 18333 en su artículo 19 específico a la salud autoriza el acceso a todos los datos por parte de los profesionales del sector salud que prestan asistencia al paciente, bajo secreto profesional. La definición uruguaya no distingue datos comunes/sensibles, ni médicos/administrativos. El carácter confidencial de los datos implica principios organizativos de protección y secreto profesional extendidos a todo el personal del hospital, incluyendo tanto el personal médico como el personal administrativo en contacto con la historia clínica de una u otra forma.

(d) La bitácora de transacciones relativas a los datos necesitando consentimiento es la fuente de control que permite fiscalizar la aplicación de la política de consentimientos. Es absolutamente necesaria en un sistema organizativo que prevee controles, como lo es ISO/IEC 27000.

(B) Encontrar los actores IHE correspondientes con los grupos de datos personales



(1) La gestión de acceso al sistema compete al actor IHE Cross-Enterprise User Authentication (XUA), única puerta de acceso a todos los sistemas de la orquestación subsecuente, dónde cada categoría de datos necesarios a la instalación de una historia clínica conforme PDP se encuentran embedidos cada uno en un actor especializado distinto.

(a) Los consentimientos informados previos dieron lugar en IHE a un perfil de integración que especializa un tipo especial de CDA específicamente para este uso. Más sobre eso en el párrafo sobre BPPC.

(b) Los datos identificatorios tienen lugar privilegiado en IHE dentro del servidor Patient Demographic Query (PDQ). Los otros actores consultan PDQ cada vez que necesitan tal información.

(2) IHE, además, flexibiliza la gestión de datos identificatorios gracias al actor Patient Index (PIX). PIX establece la correspondencia entre varios números de índice de referencia del paciente.

En el contexto Uruguayo, dónde el número de Cédula de Identidad es, por decreto ley, el identificador para comunicación de la historia clínica entre instituciones, PIX permite respetar este requerimiento y a su vez proteger la confidencialidad gracias a la creación de identificador privado aleatorio, sin significado semántico, para vincular los pacientes con sus documentos dentro del hospital.

(c) Los Registro XDS y Repositorio XDS de documentos clínicos permiten implementar varias medidas de seguridad: Entre otros, se pueden configurar de tal forma a disociar datos identificatorios y datos (que se guardan en la metadata del documento en el registro) y datos clínicos anonimizados (guardados en el documento anonimizado, dentro del repositorio).

(d) La bitácora de transacciones relativas a los datos necesitando consentimiento se encuentra gestionada por el actor ATNA, gracias al cual se garantiza la comunicación

segura punto a punto y la bitácora centralizada de todos los eventos de todos los actores presentes en el hospital. Es la herramienta fundamental para controlar la aplicación de las reglas de confidencialidad. Abrir el acceso del paciente al listado de todos los eventos relativos a su historia clínica, incluyendo la lista de quien accedió a que información, le permite fiscalizar la confidencialidad de la misma.

(C) Flexibilidad del modelo IHE BPPC

El funcionamiento de BPPC para registrar y aplicar los consentimientos previos se compone de 4 fases¹⁹ : En primer lugar, la institución define formularios de consentimiento informado previo, identificados por Object Identifiers (OID) únicos. En segundo lugar se captura el consentimiento del paciente, escaneándolo desde un formulario papel firmado, o por formulario electrónico firmado digitalmente. No obstante, el BPPC tiene que contener tanto el texto original como su transcripción en reglas escritas en xml para ser completo. En tercer lugar, cuando un documento se agrega al repositorio, está etiquetado con el (o los) OID(s) del consentimiento correspondiente(s). Este marcado está escrito en la metadata XDS del documento por lo cual se aplica a cualquier documento sin necesidad de modificarlo. En cuarto lugar, el documento está presentado al usuario solamente si las reglas del BPPC lo permiten, tomando en cuenta las reglas y el usuario autor del pedido.

El BPPC demuestra excelente flexibilidad: puede variar en el tiempo, puede trasladarse con el documento.

IHE²⁰ indica reglas admisibles y precisa que se creará un APPC (Advanced Patient Privacy Consent) cuando HL7 habrá terminado el vocabulario correspondiente. No detectamos casos no cubiertos por reglas que se puedan crear.

(C) Casos de uso

(4) Caso médico de otra institución

El acceso a los datos sigue un flujo lineal pasando varias etapas sucesivas, cada una definida por las reglas de negocio propias de actores IHE diferentes:

- Una etapa preliminar obligatoria en todos casos consiste en identificar, autenticar y averiguar los permisos del usuario del sistema de información IHE XUA (Cross-Enterprise User Authentication).

- Luego, con la ayuda del padrón IHE PDQ (Patient Demographic Query) se pide al usuario sobre que paciente quiere información.

- La consulta permite eventualmente encontrar el paciente y luego sus documentos, gracias a la equivalencia de identificador proporcionada por el servidor PIX. Se cargan entonces las reglas definidas en los consentimientos previos del paciente y guardadas en documentos BPPC (Basic Patient Privacy Consent).

- En función de los permisos del usuario y de las reglas definidas en los consentimientos previos del paciente, continuará la búsqueda de documentos, o no. En la hipótesis que continúe, se accede otra vez al Registro XDS (Cross-Enterprise Document Sharing) con el fin de brindar una lista de los documentos disponibles correspondientes al pedido del usuario.

- Finalmente, el usuario pide copia desde el repositorio XDS (Cross-Enterprise Document Sharing) de uno o varios de los documentos presentados. Si el usuario viene de afuera de la institución, se le entrega con el documento los BPPC correspondientes, que el tendrá que respetar en caso de agregar el documento a su propio repositorio.

(5) *Caso del paciente, familiar, médico de cabecera, personal administrativo de la institución de afiliación del paciente.*

Se transita el mismo flujo como con el médico externo, entre otros para poder contemplar el "derecho de no saber" ya mencionado.

Pero además se abren privilegios de acceso a la selección de los eventos relativos a los documentos del paciente, lo que garantiza el derecho de fiscalizar las creación, enmienda y uso de los documentos del paciente por el mismo.

(6) *Caso acceso científico*

Dentro del repositorio, los documentos pueden guardarse de-identificados (3) usando una técnica presentada por estudiantes del Hospital Maciel en Montevideo y reintegrar la identificación exclusivamente en la copia de los datos clínicos entregada a un usuario dentro de un contexto asistencial.

Esta separación por defecto permite establecer para acceso científico un flujo muy diferente a los otros, dado que se abre acceso directo al repositorio exclusivamente, pues solo brinda datos clínicos sin posibilidad de obtener los identificadores correspondientes.

Dado que varios repositorios pueden estar vinculados con un solo registro común y centralizado, se puede crear repositorios por especialidades, disminuyendo así la masa de datos a analizar a la ocasión de estadísticas específicas.

V.

CONCLUSIONES

IHE XDS tiene una arquitectura basada en el almacenamiento y transmisión de documento CDA desde un repositorio. Facilita el acceso a los documentos gracias a metadata guardada dentro de un registro. Esta combinación permite una excelente disociación de los datos identificatorios de un lado y datos clínicos del otro.

El modelo de documento CDA específico "BPPC" (Basic Patient Privacy Consent), por su flexibilidad, permite adaptación a los casos más complejos. La posible presencia dentro del BPPC de ambos un formulario papel firmado escaneado y de las reglas correspondientes escritas en xml, permite continuar con la práctica habitual de la firma de documentos papel y alimentar un motor automático de aplicación de las reglas de confidencialidad.

IHE XDS permite cumplir con las leyes de PDP argentinas y uruguayas, y también con ISO/IEC 27002 y ISO/IEC 27799 que definen principios de sistemas de seguridad y son pre-condiciones al respecto de las leyes de PDP.

IHE XDS conlleva los beneficios adicionales de brindar toda la documentación necesaria para el sistema de gestión de la seguridad de la información.

En conclusión, IHE XDS es un modelo a considerar muy seriamente al momento de aplicar PDP a la historia clínica.

VI.

REFERENCIAS

¹ AR: ley 25.326 (2000-08-..) accedido el 2010-02-11 desde <http://www.protecciondedatos.com.ar/ley25326.htm> y decreto correspondiente 1558/2001 (2001-...-..) accedido el 2010-02-11 desde <http://www.protecciondedatos.com.ar/dec1558.htm>

² UY: ley 18.331(2008-11-07) accedido el 2010-02-11 desde <http://www.datospersonales.gub.uy/sitio/Leyes/Ley-18.331.pdf> y decreto 414/009 (2009-08-31) accedido el 2010-02-11 desde <http://www.datospersonales.gub.uy/sitio/decretos/Decreto-414-009.pdf>

³ AR, ley 26529 (2009-11-19) accedido el 2010-02-11 desde <http://www.actualidadjuridica.com.ar/aj/lo.php?m=3&f=4&id=4375> UY, ley 18.335 (2008-08-26) accedido el 2010-02-11 desde <http://200.40.229.134/leyes/AccesoTextoLey.asp?Ley=18335>

⁴ AR, PDP Art.2, UY; PDP Art 4.E

⁵ AR, PDP Art.7; UY, PDP Art.18

⁶ AR, PDP Art.5; UY, PDP Art.18

⁷ AR, PDP Art.8; UY, PDP Art.19

⁸ AR, PDP Art.5; UY, PDP Art.9

⁹ AR, Art.11; UY, Art .17

¹⁰ AR, Art.12; UY, Art .23

¹¹ AR, Ley 25.326 Art.9; UY, Decreto 414/009 Art.7

¹² <http://www.arcert.gov.ar/politica/>

¹³ http://www.cert.uy/capacitacion/pdf/AGESIC_Buenas_practicas_en_Seguridad_de_la_Informacion.pdf

¹⁴ 27799:2008(E) 7.4.2.1

¹⁵ 27799:2008(E) 7.9.2

¹⁶ 27799:2008(E) 7.9.2.1

¹⁷ ISO 27799:2008(E) 7.7.10.2

¹⁸ UY, ley 18335, capítulo V, art.18B

¹⁹ <http://wiki.ihe.net/index.php?title=BPPC>

²⁰ <http://wiki.ihe.net/index.php?title=BPPC>