**PROYECTO:**

**CONTROL DE ACCESOS**

**(ENTREGABLE)**

**INTEGRANTES:**

201000091 – GABRIELA ROJAS MUNIVE

200921266 – AUGUSTO SUAREZ GUTIERREZ

* ENRIQUE OROSCO OSORES
* ISRAEL ANGULO CAVERO
* CARLOS CHOIS PIMENTEL

**ASIGNATURA:**

**AUDITORIA Y SEGURIDAD DE SISTEMAS**

**SECCIÓN:**

**Lima, Febrero del 2013**

# 

# RESUMEN

**HOJA DE CONTROL DE VERSIONES**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Versión** | **Item** | **Aspecto cambiado** | **Razones** | **Responsable del cambio** | **Fecha** |
| 1.0 |  | Documento original | Avance de Proyecto | Gabriela Rojas | 04/03/2013 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Gabriela E. Rojas | Gabriela E. Rojas | Gabriela E. Rojas |
| Elaborado por | Revisado por | Aprobado por |

# 

# INDICE

[RESUMEN 2](#_Toc350235701)

[INDICE 4](#_Toc350235702)

[1. PIN, SISTEMAS INTEGRALES: PARA NEGOCIOS 5](#_Toc350235703)

[2. TARJETAS SMART CARDS, RUSCO, RFID (RADIO FRECUENCIA), FIRMA DIGITAL 5](#_Toc350235704)

[3. COMPORTAMIENTO (FIRMA PERSONAL) Y FISIOLÓGICOS (SISTEMAS BIOMÉTRICOS) 5](#_Toc350235705)

[4. REGULACIONES INTERNACIONALES Y PERUANAS SOBRE SISTEMAS DE IDENTIFICACIÓN, PROTECCIÓN DE DATOS 5](#_Toc350235706)

[4.1 Normativa de Seguridad ISO/IEC 17799 5](#_Toc350235707)

[4.2 Decreto Ley 199 / 99 y la Resolución 1 del Ministerio del Interior 5](#_Toc350235708)

[4.3 DECRETO LEY 186/98 5](#_Toc350235709)

[4.4 Ley Orgánica 15/1999 5](#_Toc350235710)

[4.5 Real Decreto 994/1999 5](#_Toc350235711)

[4.6 Reglamento, COBIT y UNE-ISO/IEC 17799 5](#_Toc350235712)

[4.7 LEY 27269: Ley de Firmas y Certificados Digitales (Modificatoria en LEY 27310) 5](#_Toc350235713)

[4.8 LEY 29733: Ley de Protección de Datos Personales 6](#_Toc350235714)

[5. CASOS DE ÉXITO 6](#_Toc350235715)

[5.1 Casos de éxito GS1 RFID/EPC Transporte y Distribución Inteligente 6](#_Toc350235716)

[5.2 Exitoso Sistema Biométrico en Notarias de Lima. 7](#_Toc350235717)

[5.3 El DNI electrónico le dice 'adiós' a demoras en los servicios del Estado 8](#_Toc350235718)

# 

## PIN, SISTEMAS INTEGRALES: PARA NEGOCIOS

## TARJETAS SMART CARDS, RUSCO, RFID (RADIO FRECUENCIA), FIRMA DIGITAL

## COMPORTAMIENTO (FIRMA PERSONAL) Y FISIOLÓGICOS (SISTEMAS BIOMÉTRICOS)

## REGULACIONES INTERNACIONALES Y PERUANAS SOBRE SISTEMAS DE IDENTIFICACIÓN, PROTECCIÓN DE DATOS

## 4.1 Normativa de Seguridad ISO/IEC 17799

(Código de buenas prácticas, para el manejo de seguridad de la información) Estándar o norma internacional que vela por que se cumplan los requisitos mínimos de seguridad, que propicien un nivel de seguridad aceptable y acorde a los objetivos institucionales desarrollando buenas prácticas para la gestión de la seguridad informática.

## 4.2 Decreto Ley 199 / 99 y la Resolución 1 del Ministerio del Interior

## 4.3 DECRETO LEY 186/98

## 4.4 Ley Orgánica 15/1999

## 4.5 Real Decreto 994/1999

## 4.6 Reglamento, COBIT y UNE-ISO/IEC 17799

## 4.7 LEY 27269: Ley de Firmas y Certificados Digitales (Modificatoria en LEY 27310)

**Artículo 1º.- Objeto de la ley**

La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

**Artículo 2º.- Ámbito de aplicación**

La presente ley se aplica a aquellas firmas electróncas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

**DE LA FIRMA DIGITAL**

**Artículo 3º.- Firma digital**

La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

**DEL TITULAR DE LA FIRMA DIGITAL**

Artículo 4º.- Titular de la firma digital

El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

**DE LOS CERTIFICADOS DIGITALES**

**Artículo 6º.- Certificado digital**

El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

## 4.8 LEY 29733: Ley de Protección de Datos Personales

**Artículo 1°.- Objeto de la Ley**

La presente ley tiene por objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

**Resumen:**

Esta ley esta referida al manejo y funcionamiento de los bancos de datos personales de la administración pública y bancos privados que desarrollan sus actividades en el territorio nacional.

Los datos personales sólo pueden ser objeto de tratamiento con el consentimiento de sus titulares. En el caso de datos sensibles, se requiere consentimiento por escrito, siendo posible que se revoque la autorización brindada en cualquier momento.

No se requiere consentimiento, entre otros, en los siguientes casos:

* Datos recopilados por entidades públicas en el ejercicio de sus funciones.
* Datos que formen parte de fuentes accesibles al público.
* Datos sobre la solvencia patrimonial y de crédito.
* Cuando exista una norma para la promoción de la competencia en los mercados regulados.
* Datos necesarios para contratos, cuando el titular sea parte de ellos o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
* Datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, o cuando medien razones de interés público o de salud pública.
* Cuando el tratamiento sea efectuado por organismos sin fines de lucro.
* Cuando se hubiera aplicado un procedimiento hacer anónimos los datos o disociarlos de sus titulares.
* Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular.

## CASOS DE ÉXITO

## 5.1 Casos de éxito GS1 RFID/EPC Transporte y Distribución Inteligente

Piloto: Visibilidad de la cadena de LG a través de RFID

Las evaluaciones de uso de RFID/EPC han ido más allá de la factibilidad de la lectura, en especial cuando los proyectos compiten con su rentabilidad. El proceso de inversión en proyectos requiere resolver una necesidad operativa, y contar con un retorno económico visible. Es por eso que el retorno de la introducción de RFID en la gestión es más importante que sus costos.



Esta es la nueva cara integrada de los proyectos de RFID/EPC, en la que antes de evaluar un modelo de generación de valor, es necesario revisar los procesos e identificar como RFID impacta en las actividades para darle valor a la organización.

Dentro de esta filosofía, GS1 Perú desarrolló con Dinet un modelo de valor para la operación de la distribución de LG usando RFID utilizando la codificación estándar de GS1 y la arquitectura de intercambio de información a través de herramientas como EPC, GTIN y EDI.

## 5.2 Exitoso Sistema Biométrico en Notarias de Lima.

El Decano del Colegio de Notarios de Lima, Dr. César Bazán Naveda, indico que el Sistema Biométrico está dando auspiciosos resultados, lo que permitirá que los niveles de falsificación bajen considerablemente.



Además dijo, por ello, el CNL está ejecutando y desarrollando diversos métodos y sistemas para evitar las suplantaciones de identidades y la falsificación de documentos, como son el mencionado Sistema Biométrico de Huellas Digitales, el Sistema de Verificación de Huellas y Firmas de Notarios (SIGILLUM) y la novedosa Firma Digital y Electrónica del Papel Notarial.

En lo concerniente al Sistema Biométrico de Huellas Digitales se ha demostrado su eficacia en tres casos comprobados. Un primer caso de relevancia es el ocurrido en la notaría del Dr. Elvito Rodríguez, donde se acercaron dos personas con la intención de obtener un permiso de viaje para una menor de tan solo un año de edad, con el fin que pueda salir del país hacia Canadá. Al contrastarse sus identidades con el Sistema no existía coincidencia, por lo que se evitó que el trámite fuera realizado.

## 5.3 El DNI electrónico le dice 'adiós' a demoras en los servicios del Estado

La realización de trámites desde cualquier lugar del mundo a cualquier hora será posible con este documento. También servirá como monedero electrónico gracias a sus quince dispositivos de seguridad.

El DNI con chip, una de las grandes apuestas para la implementación del Gobierno Electrónico en el país, promete enterrar la engorrosa pérdida de tiempo y desplazamientos para completar trámites financieros, de propiedad, constitución de empresas y pago de servicios.

A estos servicios también se sumarán la obtención de certificados de antecedentes policiales, renovación de pasaportes, acceso a servicios de salud, monedero electrónico e incluso hacer transacciones relacionadas al comercio exterior.

En mayo, el Reniec anunció que los nuevos DNI con chip estarán disponibles para las personas naturales a partir del segundo semestre de este año. Sin embargo, aún queda pendiente la aprobación de los estándares de procesos digitales a cargo de Indecopi.

**Máxima seguridad**

Jorge Luis Yrivarren, jefe nacional del Reniec, aseguró que el DNI electrónico (DNIe) será una tarjeta de policarbonato con tecnología de impresiones múltiples. En el ancho de tarjeta, aunque muy delgado, se encuentran varias capas que lo hacen (casi) infalsificable.

Con el actual DNI, por ejemplo, una de las adulteraciones más comunes es el cambio de fotografía. Aun así, esta alteración es “reconocible fácilmente”, según Yrivarren, ya que la foto viene con una serie de incrustaciones numéricas irrepetibles.



Así, el funcionario indicó que “tendrían que destruir el DNI para acceder a la superficie donde se ha hecho las grabaciones”. Una de las razones es que este documento contará con 15 dispositivos de seguridad, incluyendo el uso de tecnología biométrica, que permitirá identificar al portador al momento de validar peticiones de servicios.

¿Cómo se usará este nuevo DNI? Reniec brindará una serie de equipos junto con el DNIe: lectora de chip y un software para poder habilitar las firmas digitales en los documentos (para usarse en la computadora personal), que serán usados para trámites del Estado, en primera instancia.