# Diseño de un modelo para el respaldo contingencia, recuperación y aseguramiento de la información de los procesos administrativos en la Registraduría Nacional del Estado Civil[1]


## Resumen

Con el presente trabajo se pretende ofrecer a la oficina de informática, mediante un modelo de directrices que permitan controlar la información, asegurar su integridad y mejorar su disponibilidad desarrollando un esquema de seguridad a nivel de software, hardware, redes y comunicaciones. Los resultados de esta evaluación ayudan a orientar y a determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes a seguridad de la información, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos.



***Palabras clave:*** tecnologías de información, Registraduría Nacional, estado civil, norma ISO, procedimientos y estándares de seguridad de la información.



Autor
Nelson Enrique Duarte Muñoz[2]

Director
Guillermo Hurtado


## 1. Introducción

La información relacionada con el proceso administrativo de la Registraduría Nacional representa un elemento primordial en el desempeño de la función pública, es un recurso que genera valor y es una obligación su aseguramiento y protección. Actualmente se tiene una política de backups que no ha sido llevada en su totalidad y no abarca algunos procesos que son indispensables para su función; es por esto que los procesos de información establecidos para el manejo de la información del proceso administrativo en la Registraduría Nacional requieren de planes, políticas y procedimientos que permitan la preservación de la confidencialidad, integridad y disponibilidad de la información mediante un enfoque basado en la metodología de gobernabilidad de tecno-

1 Ingeniería en redes de computadores.


2 Tecnólogo en sistematización de datos e ingeniero en redes de computadores, e-mail: ing.nduarte@gmail.com.

logías de la información, la cual especifica la librería ITIL para gestión de servicios de tecnología.

## 2. Contenido

### 2.1 Administración de riesgos

El proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información. Todas las actividades de análisis de riesgo presentadas hasta ahora tienen un solo objetivo: ayudar a desarrollar una estrategia para tratar los riesgos. Una estrategia eficaz debe considerar tres aspectos:

- Evitar el riesgo.
- Supervisar el riesgo.
- Gestión del riesgo y planes de contingencia.

Si un equipo de software adopta un enfoque proactivo frente al riesgo, evitarlo es siempre la mejor estrategia. Esto se consigue desarrollando un plan de reducción del riesgo.

### 2.2 Amenazas

Existe una relación directa entre amenaza y vulnerabilidad a tal punto que si una no existe, la otra tampoco. Las amenazas se pueden catalogar según el entorno en el cual operan:

- Amenazas del entorno (que afectan la seguridad física).
- Amenazas del sistema (que afectan la seguridad lógica).
- Amenazas de la red (que afectan las comunicaciones).
- Amenazas de personas (*insiders-outsiders*)

### 2.3 Estrategias de seguridad

Las estrategias pueden ser de dos tipos:
**Proactiva.** Se centra en reducir al mínimo los riesgos presentes en el sistema.

**Reactiva.** Se centra en una evaluación de consecuencias y daños a fin de realizar actividades de restauración del sistema y corrección de fallas.

Cuando se habla de seguridad informática se cumple literalmente:

- *Lo que no se permite expresamente está prohibido.*
- *Lo que no se prohíbe expresamente está permitido.*

En los procesos administrativos se determinan una serie de planes, políticas y procedimientos para reducir los riesgos mencionados. Para cada una de las fases de los riesgos se determina qué tipo de documento se va a utilizar para minimizar el riesgo en donde los procesos administrativos apliquen.

La Registraduría Nacional del Estado Civil en su Gerencia de Informática se divide en tres departamentos como lo son:

- Desarrollo y Programación
- Integración y Gestión
- Operaciones y Comunicaciones.

En este orden se indican, a continuación, cuáles son los servicios que la oficina de Informática presta a los procesos administrativos.

***Desarrollo y programación***

| |
|---|
| Aplicaciones |
| Mantenimientos correctivos |
| Mantenimientos evolutivos |
| Criptografía |
| Peticiones y consultas |

***Integración y gestión***

| |
|---|
| Seguridad de personal |
| Gestión de usuarios |
| Confidencialidad de información |
| Responsabilidad de usuario |

### *Operación y comunicaciones*

Copias de seguridad
Copias de host
Instalación y mantenimiento de equipos
Seguridad perimetral
Inventario de equipos y software
Soporte a continuidad de negocio
Transmisión ficheros
Instalación y mantenimiento software en clientes
soporte técnico a la operación
Líneas comunicación
Acceso internet
Gestión red
Correo
Acceso aplicaciones
Almacenamiento
Backups
Antivirus
Base de datos
Impresión
Gestión de servidores
Responsabilidad de equipo
Licenciamiento
Administración

En los procesos administrativos se determinan una serie de planes, políticas y procedimientos para reducir los riesgos mencionados.

## 2.4 Diseño de la solución

Para cada una de las fases de los riesgos se determina qué tipo de documento se va a utilizar para minimizar el riesgo en donde los procesos administrativos apliquen, teniendo en cuenta los servicios mencionados anteriormente.

### *2.4.1 Desarrollo y programación*

- Política de tercerización de aplicaciones.
- Política de aprobación de un sistema.
- Política de validación y seguridad en las aplicaciones.
- Política de cifrado, controles criptográficos y firma digital de la información.
- Política de seguridad en los sistemas de aplicaciones.
- Procedimiento de control de cambios.
- Plan de contingencia en sistema de aplicaciones.

### *2.4.2 Integración y gestión*

- Política del personal.
- Acuerdos de confidencialidad.
- Términos y condiciones de empleo.
- Plan de formación y capacitación de usuarios en materia de seguridad.
- Procedimientos de comunicación de tipos de incidentes.
- Procedimiento de comunicación de incidentes relativos a seguridad.
- Procedimiento de comunicación de debilidades en materia de seguridad.
- Procedimiento de comunicación de anomalías de software.
- Política de protección de datos y privacidad de la información personal.
- Estrategia de foro gerencial de seguridad (contiene las metodologías a usar, monitoreo de incidentes, asignación de responsabilidades, autorizaciones de seguridad).

### *2.4.3 Operaciones y comunicaciones*

- Política de resguardo de la información.
- Procedimiento de copias de seguridad.
- Plan de contingencia y recuperación de la información.
- Política de seguridad y mantenimiento del equipamiento.
- Política de áreas seguras.
- Política de control de activos.
- Plan de inventario de activos.
- Procedimiento de manejo de contraseñas.
- Política de licenciamiento y derechos de propiedad intelectual.

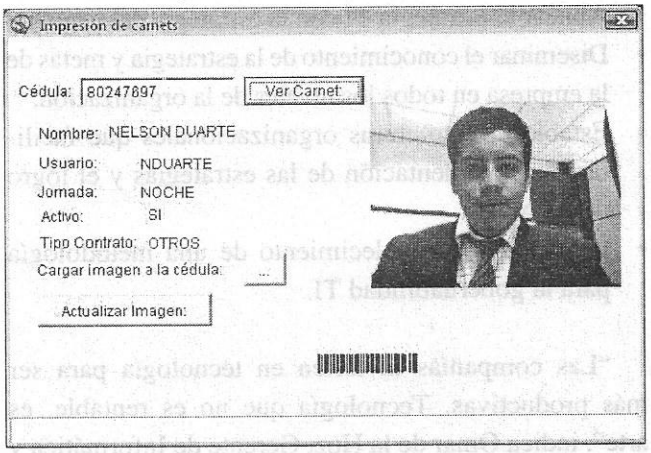
- Política de control de accesos.
- Políticas de administración de continuidad de negocio.
- Plan de contingencia a continuidad de negocio.
- Técnicas para garantizar la continuidad de negocio.
- Política de intercambios de información y software.
- Procedimientos operativos y de control de cambios en las operaciones.
- Plan de contingencia en manejo de incidentes.
- Políticas de transferencia de software desde el estado de desarrollo al estado operativo.
- Plan de separación de funciones (separar lo de desarrollo de lo operativo).
- Política de control de accesos a internet.
- Política de control de accesos a la red.
- Política de utilización de servicios de red.
- Política de mantenimiento de red.
- Política de administración de la red.
- Plan de contingencia de servicios de red.
- Procedimiento de conexión de terminales.
- Políticas de seguridad en correo electrónico.
- Procedimientos para la administración de medios informáticos.
- Procedimientos de manejo de la información (según su clasificación documentos, archivos, sistemas informáticos, redes).
- Plan de capacidad y aprobación de sistemas.
- Política de controles de software malicioso.
- Políticas de acceso público.

## 2.5 Simulación del diseño

Esta simulación permite implementar algunas de las políticas que fueron definidas en el proyecto y algunos mecanismos que determinan las buenas prácticas en el aseguramiento de la información.

Aparecerá un formulario en el que se pretende organizar según la política de control de accesos, la identificación de las personas ajenas a la Registraduría Nacional que busquen ingresar al centro de cómputo.

La segunda parte de la simulación presenta un video donde se muestra la implementación de un sniffer que




según la política de mantenimiento y gestión de red, permite medir y controlar el tráfico de la red, los servicios y administrar los equipos en la red.

## 2.6 Marco teórico

### *2.6.1 Gobernabilidad de TI*

La gobernabilidad de las tecnologías de información, o gobernabilidad TI, es un subconjunto de la disciplina gobernabilidad corporativa enfocada a los sistemas correspondientes a las tecnologías de información y a la gestión de su performance y riesgos.

¿Qué beneficios ofrece a una empresa la gobernabilidad TI?

Es reconocido que las TI son esenciales para manejar las transacciones, la información y el conocimiento necesario para ejecutar y sostener actividades económicas y sociales. Estas actividades cada vez son más globalizadas y requieren de la colaboración entre distintas entidades para ser satisfactorias. Por consiguiente, las TI son parte fundamental para soportar, sustentar y hacer crecer los negocios.

Mientras muchas empresas están de acuerdo con los beneficios potenciales que les pueden dar las TI, las empresas exitosas son las que logran asociados a la implementación de nuevas tecnologías. Para obtener los beneficios, los desafíos y preocupaciones que las empresas deben considerar son:

- Alinear la estrategia TI con la estrategia del negocio.
- Diseminar el conocimiento de la estrategia y metas de la empresa en todos los niveles de la organización.
- Establecer estructuras organizacionales que faciliten la implementación de las estrategias y el logro de las metas.
- Insistir en el establecimiento de una metodología para la gobernabilidad TI.

"Las compañías invierten en tecnología para ser más productivas. Tecnología que no es rentable, es arte", indica Omar de la Hoz, Gerente de Informática y Tecnología de Carulla Vivero. Esta frase es contundente para dimensionar la relación directa entre tecnología y productividad. No es una opción, es una exigencia para los directivos en tecnología generar productividad haciendo el mejor uso de las soluciones tecnológicas, sacándoles el mayor provecho, logrando satisfacer las necesidades de la empresa y generando valor.

## 3. Resultados obtenidos

La identificación y formulación de planes, procedimientos y políticas para el respaldo y la contingencia de la información de la Registraduría Nacional, asegura la integridad y disponibilidad de sus procesos administrativos.

La definición del modelo que se presenta al interior de este trabajo, permite proteger y asegurar la información de los procesos administrativos de la Registraduría Nacional, mediante la futura implementación de unas políticas de recuperación, de configuración, de administración y de los procedimientos de aseguramiento de la información.

## 4. Perspectivas

En aras de garantizar la integridad y la seguridad de los procesos de gestión y administración de la seguridad en la Registraduría Nacional, cada vez más ha tomado importancia el tema de la definición de procesos para el respaldo, la contingencia, la recuperación y aseguramiento de la información de sus procesos administrativos. En este sentido se ha logrado identificar la necesidad de seguridad en las diferentes aplicaciones que maneja la Registraduría Nacional y relacionadas con:

- Transacciones de información.
- Correo electrónico.
- Acceso a bases de datos confidenciales.
- Relaciones entre entidades.
- Relaciones con el Estado (Gobierno en línea).
- Intercambio de información sensible o crítica.
- Autenticación de usuarios que tienen acceso a información sensible o crítica.

Así, las soluciones que ha venido realizando la Registraduría Nacional permiten la implementación adecuada de un conjunto de garantías de seguridad técnica, basadas en la aplicación de las tecnologías de autenticidad de las transacciones, las comunicaciones realizadas, la integridad y la confidencialidad del flujo de información que se establece en cada uno de estos procesos.

## 5. Conclusiones

Entender y reconocer que la Registraduría Nacional depende cada vez más de la informática para alcanzar sus objetivos organizacionales mediante la implementación de la metodología ITIL, y de servicios informáticos de calidad que se correspondan con los objetivos de la organización, que satisfacen los requisitos y las expectativas de sus usuarios, permitiendo adicionalmente la disponibilidad de la información en caso de fallos o modificaciones necesarias, que se apoyan en los procesos de mantenimiento y operación.

## 6. Referencias

**Comité: Técnicas de Seguridad en Tecnologías de la Información.** (2006). *Normas Técnicas Iso/Iec 17799.* Bogotá: Instituto Colombiano de Normas Técnicas y Certificación, Icontec.

## 7. Referencias web

http://www.itgovernance.co.uk [Consulta: 2008, primer semestre].