RESUMEN EJECUTIVO

PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001: 2005

PRESENTADO POR:

CAREM GYSSELL NIETO GARCÍA

TUTOR ASIGNADO:

ANTONIO JOSE SEGOVIA HENARES

UNIVERSIDAD OBERTA DE CATALUNYA

MASTER INTERINSTITUCIONAL EN SEGURIDAD DE LA INFORMACION Y LAS TELECOMUNICACIONES

BARCELONA, ESPAÑA

2013

TABLA DE CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

1. MOTIVACION DEL PROYECTO

La organización para la que se realizó el Plan de Implementación de la ISO/IEC 27001: 2005 es un establecimiento público que trabaja por el desarrollo y la protección integral de la primera infancia, la niñez, la adolescencia y el bienestar de las familias en Colombia la cual está con la firme intención de cumplir con los estándares de seguridad para proteger la integridad, confidencialidad e integridad de la información que maneja y razón por la cual está en proceso de certificación de la Norma ISO 27001.

Pariendo de esta intención de certificación se seleccionó esta organización para realizar el Plan de Implementación de la ISO/IEC 27001: 2005, de tal forma que se conozca su estado actual de seguridad y se planteen las acciones para minimizar los riesgos a los que se enfrenta.

Para llegar a esto se trabajaron las siguientes fases durante el proyecto:

- Documentación normativa sobre las mejores prácticas en seguridad de la información: en la que se hace referencia a las normas ISO 27001 y 27002.
- **Situación actual:** constituye un análisis diferencial, el alcance y objetivos del plan de implementación.
- **Sistema de gestión documental:** en el que se hace referencia a las metodologías utilizadas y políticas de la organización en cuanto a seguridad.
- **Análisis de Riesgos:** contiene toda la metodología de análisis de riesgos y su desarrollo: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.
- **Propuesta de proyectos:** Corresponde al plan de implementación de controles para mitigar riesgos, contemplando recursos económicos y de tiempo.
- Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2005: se evalúan los controles, madurez y nivel de cumplimiento.
- **Presentación de resultados e informes:** presentación de los resultados del análisis, informes y presentación ejecutiva a la alta dirección.

2. ENFOQUE DEL PROYECTO

El proyecto está enfocado a proporcionar el estado actual de seguridad y planteamiento de soluciones ante los riesgos a los que se expone una organización que maneja información de carácter confidencial de niños, niñas, adolescentes y familias de Colombia. Esto específicamente en lo relacionado a la administración de la infraestructura tecnológica que apoya las actividades internas que permiten a los funcionarios llevar a cabo sus labores diarias y los servicios que el establecimiento público ofrece a la ciudadanía como son: solicitud y seguimiento a tramites tales como permisos de salida del país, adopciones, peticiones y denuncias, entre otros.

El proyecto fue desarrollado bajo los estándares ISO 27001 e ISO 27002 y para el análisis de riesgos se siguió la metodología MARGERIT que consta de las siguientes fases:

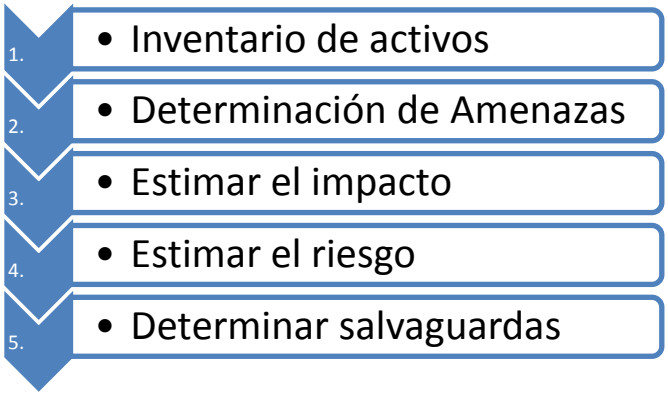

Ilustración 1 – Metodología de riesgos

Como se mencionó el análisis de riesgos se llevó a cabo para toda la infraestructura tecnológica que soporta la información de la organización y que es manejada por un contratista por lo cual se contemplan los riesgos a los que esto conlleva.

Partiendo de este análisis se determinó un plan de implementación de tal forma que se minimicen los riesgos a los que se enfrenta la organización contemplando al mismo tiempo los recursos requeridos (económicos, tiempo, humanos) para poderlo desarrollar.

Lo anterior con el propósito de:

- Identificar los riesgos a los que está expuesta la infraestructura tecnológica de la organización.

- Mantener la disponibilidad, integridad y confidencialidad de la información de los niños, niña, adolecentes, familias colombianas y demás entes que lo soliciten.

- Mejorar la seguridad actual de la organización.

3. CONLUSIONES

A continuación se listan las conclusiones más relevantes después de desarrollar el plan de implementación:

3.1. ESTADO ACTUAL DE SEGURIDAD

El estado inicial de seguridad de la información se evaluó para los 133 controles de la norma ISO 27002:2005 determinando su aplicabilidad y su porcentaje de implementación.

3.1.1. RESULTADOS ANÁLISIS DIFERENCIAL

A continuación se muestra el un gráfico con él % de aplicación de cada control como resultado del análisis diferencial:

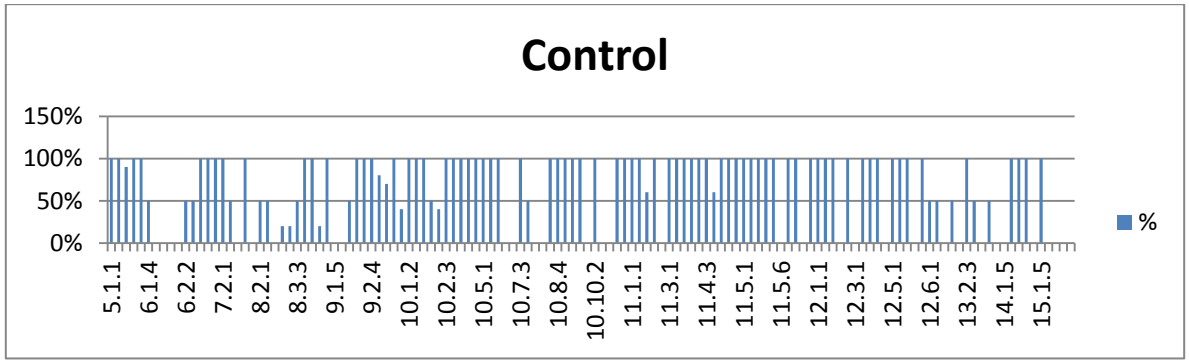

Ilustración 2- Análisis Diferencial

3.2. RESULTADOS DEL ANÁLISIS DE RIESGOS

3.2.1. VALORACIÓN DE ACTIVOS

A continuación se muestra la valoración tanto cualitativa como cuantitativa de los activos clasificados:

	Valoración		
Activo	**Valor Cualitativo**	**Total Valor**	**Valor Cuantitativo**
Equipos de almacenamiento SAN y NAS	Alta	1	300.000.000
Servidores de correo	Alta	1	100.000.000
Servidores de aplicaciones Windows	Media	0,666666667	70.000.000
Servidores de aplicaciones Linux	Media	0,833333333	70.000.000
firewall, IDS, IPS, Antispam	Alta	0,833333333	100.000.000
Equipos de backup	Alta	1	250.000.000
Equipos de networking	Alta	0,833333333	100.000.000
Controladores de dominio	Alta	0,833333333	200.000.000
Servidores de base de datos	Alta	1	200.000.000
Servidores de monitorización	Media	0,666666667	70.000.000
Especialistas	Alta	1	100.000.000

Tabla 1 - Valoración de Activos

La valoración se hizo de acuerdo a la siguiente tabla:

Valoración	Rango	Valor Cuantitativo	valor Cualitativo	CONVENCION
Alta	$100.000.000<valor>$300.000.000	$ 200.000.000	1	A
Media	$50.000.000<valor >$ 100.000.000	$ 75.000.000	0,5	M
Baja	10.000.000 <valor> $50.000.000	$ 30.000.000	0,1	B

Tabla 2 - Criterios de Valoración

Total activos: en la clasificación de activos se tuvo en cuenta un total de **11** activos y se realizó el análisis de riesgos sobre la totalidad de estos.

3.2.2. NIVEL DE RIESGOS

Para determinar el nivel de riego de los activos se tuvo como referencia la siguiente tabla:

Nivel de riesgo			IMPACTO					
			Despreciable	Muy poco frecuente	Poco Frecuente	Frecuente	Muy frecuente	Extremadamente
			0,00137	0,00273	0,005478	0,03288	0,14247	1
FRECUENCIA	Muy alto	1	0,00137	0,00273	0,005478	0,03288	0,14247	1
	Alto	0,75	0,0010275	0,0020475	0,0041085	0,02466	0,1068525	0,75
	Medio	0,5	0,000685	0,001365	0,002739	0,01644	0,071235	0,5
	Bajo	0,2	0,000274	0,000546	0,0010956	0,006576	0,028494	0,2
	Muy bajo	0,05	0,0000685	0,0001365	0,0002739	0,001644	0,0071235	0,05

Tabla 3 - Nivel de Riesgos

De tal forma que según el color definido los riesgos se clasificarían en riesgos aceptables y riesgos a tratar así:

Ilustración 3- Clasificación de riesgos

3.2.1. MAPA DE RIESGOS

A continuación se presenta el mapa de riesgos como un consolidado del análisis de riesgos:

Nivel de riesgo			IMPACTO					
			Despreciable	Muy poco frecuente	Poco Frecuente	Frecuente	Muy frecuente	Extremadamente frecuente
			0,00137	0,00273	0,005478	0,03288	0,14247	1
FRECUENCIA	Muy alto	1	0	0	0	0	0	0
	Alto	0,75	12	23	3	6	9	0
	Medio	0,5	127	18	0	5	8	0
	Bajo	0,2	0	20	0	0	0	0
	Muy bajo	0,05	0	0	0	0	0	0

Tabla 4 - Mapa de Riesgos

En resumen el total de riesgos encontrados es el siguiente:

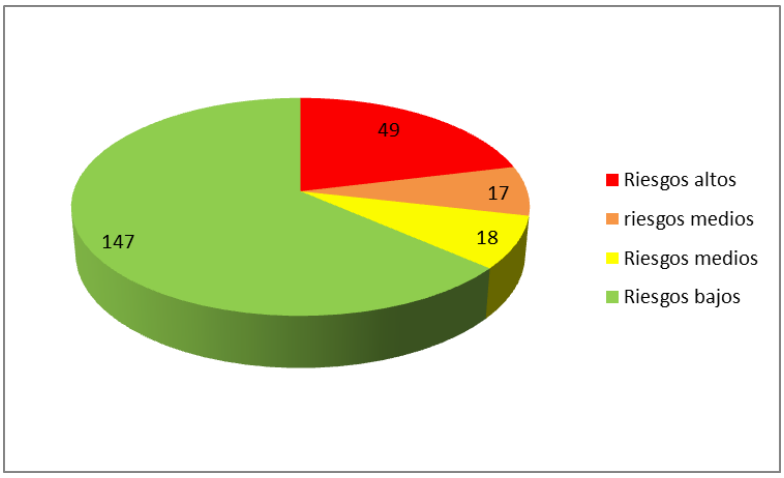

Ilustración 4 - Resumen de Riesgos

Según esto los riesgos a tratar son **49** en total y para los cuales se desarrollaron propuestas de proyectos.

3.2.2. AMENAZAS

Para el desarrollo del análisis de riesgos se tuvieron en cuenta amenazas de los siguientes tipos:

- Del entorno
- Técnicas
- Causadas por personas accidentalmente
- Causadas por personas intencionalmente

Las amenazas con las que se llevó a cabo el análisis son las siguientes:

	AMENAZAS
1	Falla de suministro de energía
2	Falla de aire acondicionado
3	Degradación de equipo informático.
4	Manipulación inadecuada del equipo informático.
5	Contaminación por polvo/polen/esporas
6	Eliminación negligente de datos
7	Ingeniería social
8	Robo de datos o documentos
9	Exposición de contraseña
10	No-disponibilidad de respaldos
11	Falla en los datos respaldados

12	Fallas no detectadas a tiempo
13	Falta de trazabilidad
14	Fallas ocasionadas por un cambio
15	Información sensible sin cifrar
16	uso inadecuado del correo
17	Software malicioso
18	Spam
19	Denegación de servicio
20	Escalada de privilegios
21	Ejecución remota de código malicioso
22	Mal uso de puertos de acceso remoto para administración/diagnóstico
23	Falla de hardware
24	Contraseñas no protegidas, claves certificados
25	Control de acceso Inadecuado
26	Déficit de personal
27	Falta de capacitación de los ingenieros de backup y de disponibilidad

Tabla 5 - Amenazas

3.3. PROPUESTAS DE PROYECTOS

Se desarrolló el plan de implementación para tratar los riesgos altos encontrados en el análisis de riesgos. A continuación las propuestas planteadas para este fin en la que se determinan las actividades a realizar, los responsables de cada actividad, el presupuesto requerido para su implementación y las fechas de implementación:

Objetivo de Control	Control	Riesgo al que aplica	Actividades	Responsable	Recursos Requeridos	Presupuesto	Fecha de Inicio de Implementación	Fecha Final de Implementación	Porcentaje de Implementación.
10.4 Protección contra el código malicioso y descargable	10.4 Protección contra el código malicioso y descargable	B17, C17, F17, G17, H17, I17, J17	* Instalar solución antispam y antimalware para exchange * Instalar antivirus a todos los servidores Windows	Especialista de Echange Oficial de Seguridad Especialista de servidores	* Instalador Fore fron for Echange. * Capacidad de Disco procesamiento y RAM en el Servidor. * Dos semanas de pruebas e implementacion * Instalador de antivirus * 1 mes para instalacion de antivirus	$ 3.000.000	1 de junio de 2013	10 de julio de 2013	0
10.6 Gestión de la seguridad de las redes.	10.6. 2. Seguridad en los servicios de red	A15, B15, C15, D15, E15, F15, G15, H15, I15, J15	1. Hacer recomendación de encripciónde datos al lider de redes WAN. 2. Cifrar la información o los canales de datos tanto de las regionales como de la sede nacional a terremark.	Especialista de redes WAN Oficial de Seguridad	* 1 Semana de prueba e implementación * Ampliación del andho de banda del canal	$ 10.000.000	1 Julio de 2013	10 Julio de 2013	0
10.10 Monitoreo	10.10. 1. Registros de auditoria	A12, A13, B13, C13, D13, E13, F13, H13, I13, J13	1. Diseñar y documentar el proceso de manejo de registros de auditoria. 2. Determinar la herramienta almacenamiento de logs centralizados. 3. Configurar los servidores cliente para redireccionar los archivos de log al servidor con la herramienta definida..	Especialista de servidores Oficial de Seguridad	* herramienta de logs * Servidor con recursos de alamacenamiento * 3 semanas para la implementación y pruebas	$ 15.000.000	1 Junio de 2013	22 de Junio de 2013	0
11.2 Gestión del acceso de usuarios	11.2.2. Gestión de privilegios	A6, A8	1. Establecer los roles y permisos que tienen los usuarios para acceder a la SAN. (Matriz de roles y privilegios). 2. Auditar los servicios Vs. Matriz de roles. 3. Impleemntar los roles definidos para el acceso a la SAN (AD)	Especialista de almacenamiento Lider de capacidad Recursos Humanos Especialista de Servidores (AD) Oficial de Seguridad	* 1 mes para la creación de la matriz *`1 mes implementacion de roles en el accesos a la SAN	$ 2.000.000	1 Junio de 2013	1 de Agosto de 2013	40
	11.2.3. Gestión de contraseñas de usuarios	I9	2. Detectar que aplicaciones no cumplen con la politica de contraseñas de aplicaciones. 4. Implementacion de contraseñas fuertes	Especialista de aservidores Oficial de Seguridad	* 1 mes para identificar aplicaciones con problemas de contraseñas	$ 2.000.000	1 Junio de 2013	1 Julio de 2013	30
11.5 Control de acceso al sistema operativo	11.5.1 Procedimientos seguros de inicio de sesión.	D25	* Crear linea base de seguridad * Aplicar una línea base de seguridad para el acceso a servidores.	Especialista de Servidores Oficial de seguridad	* 1 mes para creación de linea base * 2 meses Implementación	$ 2.000.000	1 Julio de 2013	1 Septiembre de 2013	20
	11.5.3. Sistema de gestión de contraseñas.	D24, I24	* Verificar que las contraseñas de los usuarios del sistema operativo y aplicaciones cumplan con la politica de contraseñas definida. * Las contraseñas deben permanecer en estado cifrado.	Especialista de Servidores Oficial de seguridad	* 1 mes para identificar servidores con contraseñas que no cumplen la política * 1 mes par aplicar la política	$ 2.000.000	1 Junio de 2013	1 Agosto de 2013	40
14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio.	14.1.3. Redacción e implantación de planes de continuidad	E23, F23	* Desarrollar planes de contingencia para fortimail, avamar, librería y networker. * Realizar y ejecutar un plan de capacidad de los servidores de terremak que actualmente estan en alta disponibilidad para que soporten la operación en caso de fallo.	Especualista de servidores Subdirector de recursos Informaticos Oficial de seguridad	* 2 meses para hacer el plan de contingencia y obtener recursos	$ 30.000.000	1 Julio de 2013	1 Septiembre de 2013	0

Tabla 6 - Propuestas de Proyectos

3.3.1. CONTROLES PROPUESTOS

Para mitigar los 49 riesgos se propuso la utilización de **8** de la norma ISO/IEC 27002:2005 controles correspondientes a **6** objetivos de control. A continuación los controles propuestos y los riesgos que afecta:

Objetivo de Control	Control	Riesgo al que aplica
10.4 Protección contra el código malicioso y descargable	10.4 Protección contra el código malicioso y descargable	B17, C17, F17, G17, H17, I17, J17
10.6 Gestión de la seguridad de las redes.	10.6. 2. Seguridad en los servicios de red	A15, B15, C15, D15, E15, F15, G15, H15, I15; J15
10.10 Monitoreo	10.10. 1. Registros de auditoria	A12, A13, B13, C13, D13, E13, F13, H13, I13, J13
11.2 Gestión del acceso de usuarios	11.2.2. Gestión de privilegios	A6, A8
	11.2.3. Gestión de contraseñas de usuarios	I9
11.5 Control de acceso al sistema operativo	11.5.1 Procedimientos seguros de inicio de sesión.	D25
	11.5.3. Sistema de gestión de contraseñas.	D24, I24
14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio.	14.1.3. Redacción e implantación de planes de continuidad	E23, F23

Tabla 7 - Controles

3.4. AUDITORÍA DE CUMPLIMIENTO

Después de conocer los activos de la organización y haber realizado un análisis de riesgos se llevó a cabo una auditoría para tener claro el nivel de cumplimiento en materia de seguridad. Como marco de referencia se utilizó la norma ISO/IEC 27002:2005.

3.4.1. RESULTADOS EVALUACIÓN DE LA MADUREZ

El cálculo de la madurez de la organización en cuanto a seguridad se hizo teniendo en cuenta los 133 controles de la norma ISO/IEC 27002:2005 y basándose en el modelo de madurez de capacidad (CMM) el cual da las pautas para evaluar el estado de cada control. Partiendo de esto se presentan el detalle de la evaluación de madurez:

CONTROL	Efectividad
5. Política de Seguridad	90%
5.1 Política de Seguridad de la Información	90%
5.1.1 Documento de la Política de SI	90%
5.1.2 Revisión de la Política de SI	90%
6. Organización de la SI	90%
6.1 Organización Interna	90%
6.1.1 Compromiso de la dirección con la seguridad de la información	90%
6.1.2 Coordinación de la Seguridad de la Información	90%
6.1.3 Asignación de Responsabilidades para la Seguridad de la Información	90%
6.1.4 Proceso de Autorización para los Servicios	50%
6.1.5 Acuerdos sobre Confidencialidad	10%
6.1.6 Contacto con las Autoridades	0%
6.1.7 Contacto con Grupos de Interés Especiales	0%
6.1.8 Revisión Independiente de la SI	N/A

6.2 Partes Externas	50%
6.2.1 Identificación de los Riesgos	90%
6.2.2 Seguridad con los Clientes	10%
6.2.3 Seguridad en los Acuerdos con Terceras Partes	10%
7. Gestión de Activos	90%
7.1 Responsabilidad por los Activos	90%
7.1.1 Inventario de Activos	90%
7.1.2 Propietario de los Activos	90%
7.1.3 Uso Aceptable de los Activos	50%
7.2 Clasificación de la Información	90%
7.2.1 Directrices de Clasificación	50%
Se está trabajando en conjunto con gestión documental para rotular la información.	50%
8. Seguridad de los Recursos Humanos	50%
8.1 Antes de la Contratación Laboral	50%
8.1.1 Roles y Responsabilidades	10%
8.1.2 Selección	90%
8.1.3 Términos y Condiciones Laborales	0%
8.2 Durante la Vigencia del Contrato	50%
8.2.1 Responsabilidades de la dirección	50%
8.2.2 Educación, formación y concientización sobre SI	50%
8.2.3 Proceso Disciplinario	10%
8.3 Terminación o Cambio de la Contratación	50%
8.3.1 Responsabilidades en la Terminación	10%

8.3.2 Devolución de Activos	10%
8.3.3 Retiro de los Derechos de Acceso	50%
9. Seguridad Física y del Entorno	90%
9.1 Áreas Seguras	90%
9.1.1 Perímetro de Seguridad Física	100%
9.1.2 Controles de Acceso Físico	90%
9.1.3 Seguridad de Oficinas, Recintos e Instalaciones	90%
9.1.4 Protección contra Amenazas Externas y Ambientales	90%
9.1.5 Trabajo en Áreas Seguras	90%
9.1.6 Áreas de Carga, despacho y acceso público	90%
9.2 Seguridad de los Equipos	90%
9.2.1 Ubicación y Protección de los Equipos	90%
9.2.2 Servicios de Suministro	100%
9.2.3 Seguridad del Cableado	100%
9.2.4 Mantenimiento de los Equipos	90%
9.2.5 Seguridad de los Equipos Fuera de las Instalaciones	50%
9.2.6 Seguridad en la Reutilización o Eliminación de los Equipos	50%
9.2.7 Retiro de Activos	90%
10. Gestión de Comunicaciones y Operaciones	90%
10.1 Procedimientos Operacionales y Responsabilidades	90%
10.1.1 Documentación de los procedimientos de operación	50%

10.1.2 Gestión del Cambio	100%
10.1.3 Distribución (segregación) de funciones	90%
10.1.4 Separación de las instalaciones de Desarrollo, ensayo y operación	90%
10.2 Gestión de la Prestación del Servicio por Terceras Partes	50%
10.2.1 Prestación del Servicio	50%
10.2.2 Monitoreo y revisión de los servicios por terceros	50%
10.2.3 Gestión de los Cambios en los servicios por terceras partes	90%
10.3 Planificación y Aceptación del Sistema	90%
10.3.1 Gestión de la Capacidad	90%
10.3.2 Aceptación del Sistema	90%
10.4 Protección Contra Códigos Maliciosos y Móviles	50%
10.4.1 Controles contra códigos maliciosos	50%
10.4.2 Controles contra códigos móviles	90%
10.5 Respaldo	90%
10.5.1 Respaldo de la Información	90%
10.6 Gestión de la Seguridad de las Redes	90%
10.6.1 Controles de las Redes	90%
10.6.2 Seguridad de los servicios de la red	90%
10.7 Manejo de los Medios	50%
10.7.1 Gestión de los Medios Removibles	0%
10.7.2 Eliminación de los Medios	0%
10.7.3 Procedimientos para el Manejo de la Información	90%

10.7.4 Seguridad de la Documentación del Sistema	50%
10.8 Intercambio de la Información	50%
10.8.1 Políticas y Procedimientos para el Intercambio de Información	0%
10.8.2 Acuerdos para el intercambio	0%
10.8.3 Medios Físicos en tránsito	90%
10.8.4 Mensajería Electrónica	90%
10.8.5 Sistemas de Información del Negocio	90%
10.9 Servicios de Comercio Electrónico	90%
10.9.1 Comercio Electrónico	N/A
10.9.2 Transacciones en Línea	90%
10.9.3 Información disponible al público	90%
10.10 Monitoreo	50%
10.10.1 Registro de Auditorías	10%
10.10.2 Monitoreo del uso del Sistema	90%
10.10.3 Protección de la Información del Registro	10%
10.10.4 Registros del Administrador y del Operador	10%
10.10.5 Registro de Fallas	100%
10.10.6 Sincronización de Relojes	90%
11. Control de Acceso	90%
11.1 Requisitos del Negocio para el Control del Acceso	90%
11.1.1 Política de Control de Acceso	100%
11.2 Gestión del Acceso a Usuarios	50%
11.2.1 Registro de Usuarios	100%

11.2.2 Gestión de Privilegios	50%
11.2.3 Gestión de Contraseñas para Usuarios	50%
11.2.4 Revisión de los Derechos de Acceso de los Usuarios	0%
11.3 Responsabilidades de los Usuarios	90%
11.3.1 Uso de Contraseñas	50%
11.3.2 Equipo de Usuario Desatendido	100%
11.3.3 Política de Escritorio Despejado y de Pantalla Despejada	100%
11.4 Control de Acceso a las Redes	90%
11.4.1 Política de uso de los servicios de red	100%
11.4.2 Autenticación de Usuarios para Conexiones Externas	100%
11.4.3 Identificación de los Equipos en las Redes	90%
11.4.4 Protección de los puertos de configuración y diagnóstico remoto	50%
11.4.5 Separación en las Redes	100%
11.4.6 Control de Conexión a las redes	100%
11.4.7 Control de Enrutamiento en la Red	100%
11.5 Control de Acceso al Sistema Operativo	90%
11.5.1 Procedimientos de Registro de Inicio Seguro	90%
11.5.2 Identificación y Autenticación de Usuarios	100%
11.5.3 Sistema de Gestión de Contraseñas	90%
11.5.4 Uso de las utilidades del sistema	90%
11.5.5 Tiempo de Inactividad de la Sesión	100%
11.5.6 Limitación del tiempo de Conexión	10%

11.6 Control de Acceso a las Aplicaciones y a la Información	90%
11.6.1 Restricción de acceso a la Información	50%
11.6.2 Aislamiento de sistemas sensibles	100%
11.7 Computación Móvil y Trabajo Remoto	50%
11.7.1 Computación y comunicaciones móviles	0%
11.7.2 Trabajo Remoto	100%
12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	90%
12.1 Requisitos de Seguridad de los Sistemas de Información	90%
12.1.1 Análisis y especificación de los requisitos de seguridad	90%
12.2 Seguridad de las aplicaciones del sistema	50%
12.2.1 Validación de los datos de entrada	90%
12.2.2 Control de Procesamiento Interno	90%
12.2.3 Integridad del Mensaje	0%
12.2.4 Validación de los datos de salida	90%
12.3 Controles Criptográficos	50%
12.3.1 Política sobre el uso de controles criptográficos	0%
12.3.2 Gestión de Claves	90%
12.4 Seguridad de los Archivos del Sistema	50%
12.4.1 Control del Software Operativo	50%
12.4.2 Protección de los datos de prueba del sistema	90%
12.4.3 Control de acceso al código fuente de los programas	0%
12.5 Seguridad en los procesos de desarrollo y soporte	90%

12.5.1 Procedimientos de control de cambios	90%
12.5.2 Revisión Técnica de las aplicaciones después de los cambios en el SO	90%
12.5.3 Restricciones en los cambios a los paquetes de software	90%
12.5.4 Fuga de información	0%
12.5.5 Desarrollo de software contratado externamente	90%
12.6 Gestión de la Vulnerabilidad Técnica	90%
12.6.1 Control de las Vulnerabilidades Técnicas	90%
13. Gestión de los Incidentes de la Seguridad de la Información	50%
13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información	50%
13.1.1 Reporte sobre los eventos de seguridad de la información	50%
13.1.2 Reporte sobre las debilidades en la seguridad	50%
13.2 Gestión de los Incidentes y las mejoras en las SI	50%
13.2.1 Responsabilidades y Procedimientos	50%
13.2.2 Aprendizaje debido a los incidentes de SI	0%
13.2.3 Recolección de Evidencias	50%
14. Gestión de la Continuidad del Negocio	50%
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	50%
14.1.1 Inclusión de la SI en el proceso de gestión de la continuidad del negocio	50%
14.1.2 Continuidad del Negocio y evaluación de riesgos	0%
14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la SI	10%
14.1.4 Estructura para la Planificación de la continuidad del negocio	0%

14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	0%
15. Cumplimiento	90%
15.1 Cumplimiento de los Requisitos Legales	90%
15.1.1 Identificación de la Legislación Aplicable	90%
15.1.2 Derechos de Propiedad Intelectual	90%
15.1.3 Protección de los Registros de la Organización	90%
15.1.4 Protección de los Datos y privacidad de la información personal	0%
15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de información	90%
15.1.6 Reglamentación de los controles criptográficos	N/A
15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico	0%
15.2.1 Cumplimiento con la políticas y las normas de seguridad	0%
15.2.2 Verificación del cumplimiento técnico	0%
15.3 Consideraciones de la Auditoría de los Sistemas de Información	0%
15.3.1 Controles de Auditoría de los sistemas de información	0%
15.3.2 Protección de las herramientas de auditoría de los SI	0%

Tabla 8 - Evaluación de madurez

El resumen de la madurez CCM de los controles se presenta a continuación:

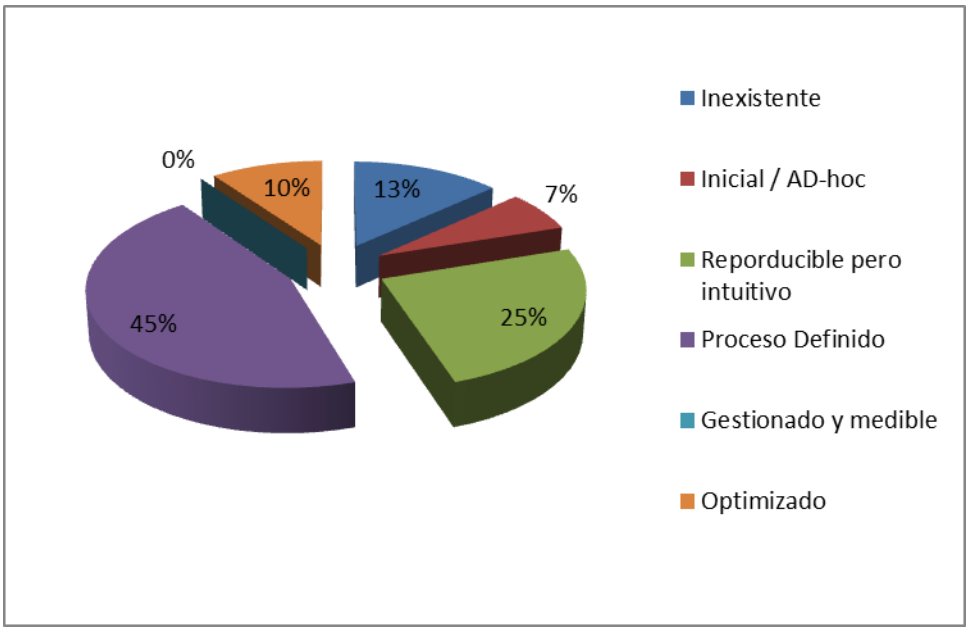

Ilustración 5 - Resumen de la Madurez CCM