INFORME FINAL DE AUDITORIA

Nivel de madures CMM para las dominios de la norma ISO/IEC 27001:2005

Telecomunicaciones

Elaborado por:

Héctor Fernando Vargas Montoya

Junio – 2014

Control de versiones del documento

Versión	Fecha	Creada por	Descripción
1.0	Abril 10 de 2014	Héctor Vargas	Creación del documento

Contenido

Lista de Figuras

Lista de tablas

1. Objetivo de la auditoria

Ésta auditoria pretende mostrar el nivel de cumplimiento de la norma ISO/IEC 27001:2005 bajo el modelo de madurez CMM, con ello, poder ver reflejado el nivel de implementación de los diferentes dominios de la norma.

2. Alcance de la auditoría

Auditoría para el SGSI, delimitado por la declaración de aplicabilidad.

3. Escalas de calificación

Los diferentes hallazgos se evaluarán de la siguiente manera:

- *No conformidad menor.*
- *No conformidad mayor.*
- *Conformidad o aceptación.*
- *Oportunidad de mejora*

4. Equipo auditor

Auditor Líder: Héctor Fernando Vargas Montoya

Equipo de apoyo: Analistas de seguridad

5. Fechas de la ejecución de la auditoria

Inicio: Mayo 19 de 2014

Fin: Mayo 28 de 2014

6. Informe ejecutivo y conclusiones

La auditoria de cumplimiento se hace sobre los 11 dominios de la norma ISO/IEC 27001:2005, evaluado bajo el modelo de madurez de capacidad CMM a los 133 controles de la norma ISO/IEC 27002:2005.

Para la evaluación de los controles de la norma ISO/IEC 27001:2005, se tomó cada uno de los controles y se calificaron acorde a la siguiente tabla:

Efectividad	CMM	Significado	Descripción
0%	**L0**	*Inexistente*	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	*Inicial / Ad-hoc*	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 1: Niveles de calificación madurez CMM

En el anexo 11 "auditoria de cumplimiento" podemos revisar el detalle de la evaluación realizada, la cual comprende los siguientes resultados:

a) Nivel de implementación basado en CMM

La siguiente tabla muestra el nivel de implementación de los controles:

ISO 27002 - DOMINIO		
Numeral	**Dominio**	**Porcentaje cumplimiento**
A.5	A.5 Politicas de seguridad	100,00%
A.6	A.6 Organización de la seguridad de la Información	60,00%
A.7	A.7 Gestión de activos	69,17%
A.8	A.8 Seguridad de los recursos humanos	65,00%
A.9	A.9 Seguridad física y ambiental	85,12%
A.10	A.10 Gestión de las comunic y oper	73,01%
A.11	A.11 Control de acceso	65,07%
A.12	A.12 Adquisición, dllo y mante. de SI	72,44%
A.13	A.13 Gestión de incidentes de seguridad de la información	90,00%
A.14	A.14 Gestión de la continuidad del negocio	67,00%
A.15	A.15 Cumplimiento	61,39%

Tabla 2: Resultado de calificación CMM

Podemos observar que todos los controles están por encima del 60%, con muy buenos resultados en 2 dominios, las políticas de seguridad y la gestión de incidentes de seguridad de la información, los cuales, se evidencia un trabajo importante.

b) Hallazgos

A continuación se presenta el resumen general por dominio de hallazgos:

Numeral	Dominio	Calificación
A.5	*A.5 Politicas de seguridad*	**Conformidad o aceptación**
A.6	*A.6 Organización de la seguridad de la Información*	**Conformidad o aceptación**
A.7	*A.7 Gestión de activos*	**Conformidad o aceptación**
A.8	*A.8 Seguridad de los recursos humanos*	**No conformidad menor** *(control A.8.3, Terminación o cambio del contrato laboral): Algunos procedimientos para el desaprovisionamiento de personal no se está ejecutando.*
A.9	*A.9 Seguridad física y ambiental*	**Conformidad o aceptación**
A.10	*A.10 Gestión de las comunic y oper*	**No conformidad menor** *(control A.10.8, Intercambio de la información): No hay un lineamiento claro y documentado sobre como es el intercambio de información con terceras partes.*
A.11	*A.11 Control de acceso*	**Conformidad o aceptación**
A.12	*A.12 Adquisición, dllo y mante. de SI*	**Oportunidad de mejora:** *Es necesario fortalecer el monitoreo en los sistemas, archivos y carpetas.*
A.13	*A.13 Gestión de incidentes de*	**Oportunidad de mejora***: Es importante contar con una*

	seguridad de la información	*herramienta más automática para el registro de incidentes.*
A.14	*A.14 Gestión de la continuidad del negocio*	**Oportunidad de mejora***: Es necesario que en la gestión de riesgos se indique cuales pueden ser las fuentes de riesgos, como los incidentes de seguridad.*
A.15	*A.15 Cumplimiento*	**Oportunidad de mejora:** *Se debe integrar las diferentes áreas para fortalecer los procedimientos hacia el cumplimiento.*

Tabla 3: Hallazgos generales de la auditoria

c) Conclusiones

Teniendo en cuenta la medición inicial con respecto a la actual (CMM), podemos observar de una forma positiva como ha mejorado la implementación de los controles de la norma, teniendo en cuenta muchas acciones de mejora de desarrollar.

No se ve una variación significativa en el dominio de cumplimiento (A.15) ni en el control de acceso (A.11), temas importantes a trabajar.

Es importante trabajar sobre las no conformidades y las acciones de mejora planteadas.

7. Informe detallado: Hallazgos y evidencias

A continuación se presentan los hallazgos encontrados durante la auditoria:

a) Tabla de hallazgos

Número Hallazgo	Hallazgo / evidencias	Riesgo	Recomendación Acción de mejora
1.	Terminación o cambio del contrato laboral (A.8.3): En algunas revisiones se encontró que empleados que ya no hacen parte de la compañía, no fueron retirados de los sistemas de información.	Acceso no autorizado, posible pérdida/extracción de información.	Ajustar y hacer seguimiento al procedimiento estipulado para dar de alta a usuarios que ya no usan el sistema o no se encuentran en la organización.
2.	Intercambio de la información (10.8): No se evidencio con claridad cómo se envía o recepciona la información que debe ser intercambiada con terceras partes. Alguna es enviada por correo y otra por sistemas seguros.	Pérdida de confidencialidad y trazabilidad sobre las comunicaciones enviadas.	Ajustar y homologar el procedimiento para intercambio de información.
3.	Seguridad de los archivos del sistema (A.12.4): No se evidencia un monitoreo fuerte para el control de software, aunque hay procedimientos no se hace un seguimiento a estos.	Instalación de software no permitido, posibilidad de infracción de derechos de autor.	Hacer seguimiento a las diferentes aprobaciones de permisos especiales sobre los sistemas.
4.	Reporte sobre los eventos y las vulnerabilidades de la seguridad de la información (A.13.1): Existen 2 varias herramientas para el registro y monitoreo de los incidentes de seguridad.	Pérdida de visibilidad del riesgos, falencia en el aprendizaje a través de incidentes de seguridad	Para una mejor trazabilidad y gestión del conocimiento de los incidentes, se debería tener una matriz unificada de reporte y documentación.
5.	Aspectos de seguridad de la información, de la gestión de la continuidad del negocio (A.14.1): Si bien se tiene un proceso de continuidad, algunas pruebas se hacen sobre plataformas y sistemas que no son el alcance de implementación.	No descubrimiento a tiempo de problemas de continuidad	Realizar pruebas de continuidad sobre el sistema de referencia.

6.	Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico (A.15.2): Existen varias áreas en la compañía que revisan los procesos de cumplimiento, en algunas ocasiones estos procedimientos no son concordantes.	Posibilidad de no implementación de controles asociados al cumplimiento.	Unificar el procedimiento de revisión de los procedimientos de validación.

Tabla 4: Detalle de hallazgos, riesgos y recomendaciones

b) Resultado según CMM

A continuación se entrega el nivel de cumplimiento, nivel de madurez CMM de la norma ISO 27002:2005:

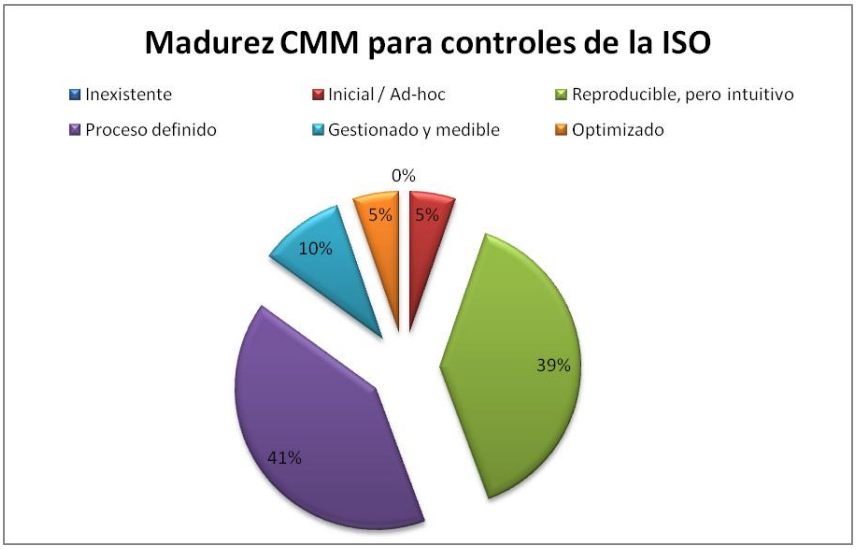

Figura 1: Resultado modelo de madurez - CMM

Vemos como, el mayor porcentaje está entre los controles que poseen un proceso definido y los que son reproducibles, pero aún intuitivo. Solo un 5% de los controles están optimizados. Es importen resaltar que no hay porcentaje para controles "inexistentes", lo que indica que el modelo de implementación, responsabilidad y de gobierno va por buen camino y hay una existencia de aprobación y respaldo por las áreas impactadas.

Ahora bien, con respecto a una medición inicial (anexo 1), hay una mejora notable y muchas oportunidades de mejora, se podría precisar que el aumento en la medición podría darse por algunos "quick wins" o ganancias tempranas que se pudieron implementar y así subir el nivel en los controles.

c) Visión de los dominios

A continuación podemos observar el nivel de madures de los 11 dominios de la norma:

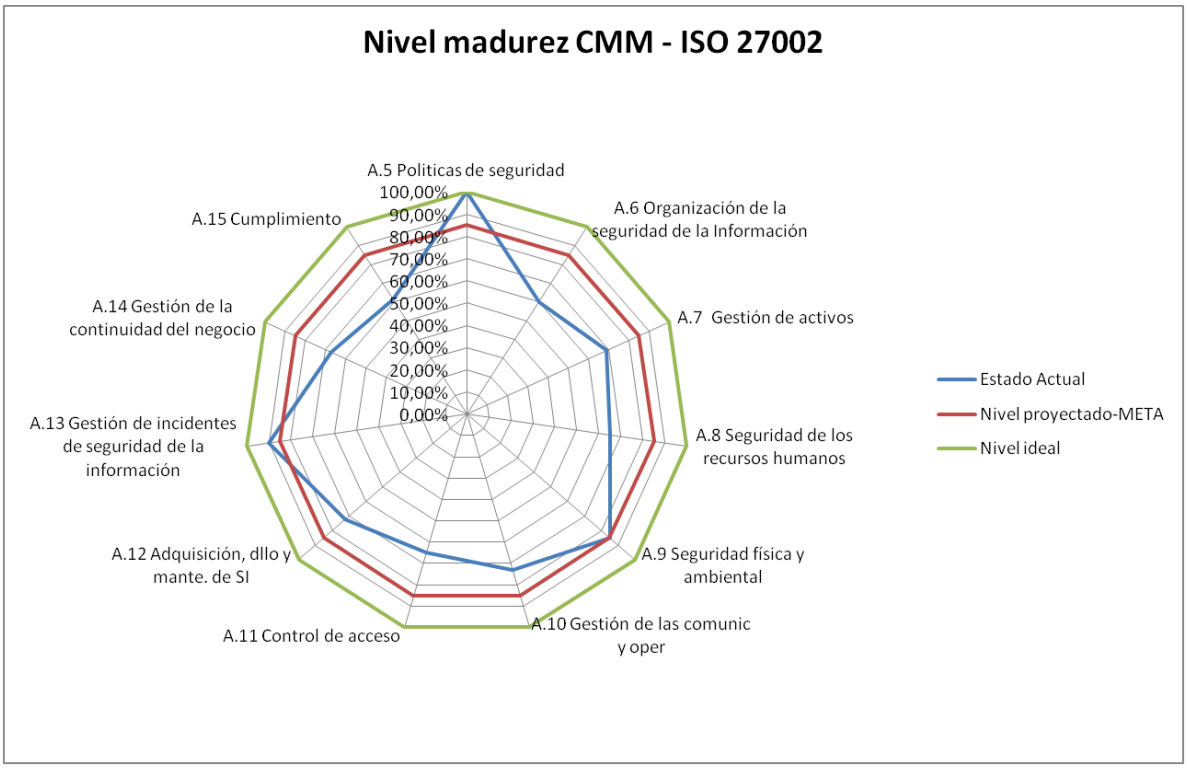

Figura 2: Resultado modelo de madurez - CMM

Es importante precisar que la medición inicial (anexo 1) tiene una escala diferente, pero aproximada, lo que implica que podríamos tener un margen de error a la hora de evaluar que tanto se ha implementado los controles y cómo ha sido la diferencia con respecto a la inicial.

d) Nivel de cumplimiento de los objetivos de control

La siguiente gráfica ilustra el estado de cumplimiento, bajo CMM, de los 39 dominios de control:

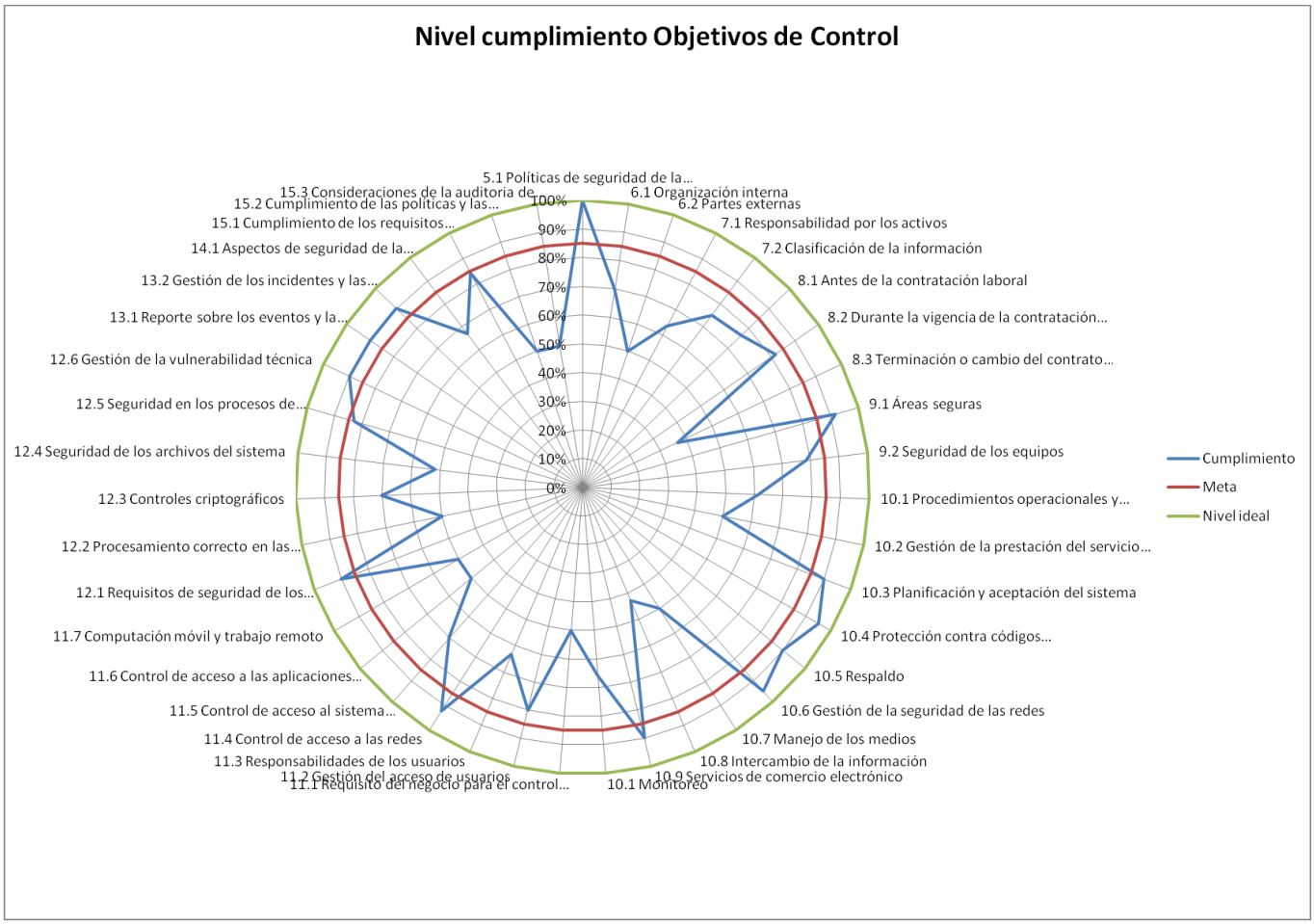

Figura 3: Resultado modelo de madurez - CMM

8. Bibliografías y fuentes de referenciación

Como fuente de referenciación tenemos:

- *Los diferentes procesos, procedimientos y soportes que al interior de la compañía se tienen, los cuales están publicados en la Intranet (o Web Corporativa).*
- *La medición inicial realizada.*
- *La gestión de riesgos realizada.*