ISO-27001 e ISO-27004

Viena 2007

Por: Alejandro Corletti Estrada
Mail: acorletti@hotmail.com

PRÓLOGO

Uno de los aspectos más importantes que se debe destacar del estándar ISO 27001, es la importancia que hace sobre el carácter "medible de los controles". En concreto, si un control no se puede medir, entonces no nos aporta absolutamente nada al SGSI (**S**istema de **G**estión de la **S**eguridad de la **I**nformación). Ahora bien, ¿Cómo debemos medir esos controles?, es aquí donde entra en juego el estándar **ISO 27004**, y como se verá en este texto, aporta un gran valor agregado en el momento de comenzar a implementar esta norma, pues desde el inicio, se comienzan a pensar todas las fases de la misma bajo el concepto de "Medición".

NOTA: Para poder comprender con claridad el sentido, los conceptos y definiciones que aquí se desarrollarán, es recomendable leer previamente los artículos que se han publicado con anterioridad respecto a esta familia de estándares, los cuales son:

- **"Análisis de ISO 27001:2005"**
- **"ISO-27001: Los controles (Parte I)"**
- **"ISO-27001: Los controles (Parte II)"**

PRESENTACIÓN

Al igual que el ISO 27001, esta norma (que aún se encuentra en estado de borrador) tiene como responsable al **JTC 1** (Join Technical Committee Nº1) JTC 1 y dentro de él, al subcomité **SC 27**, IT "Security Techniques"

Luego del plenario en Malasia del 07 de noviembre del 2005, se inició la circulación de este documento para estudio y comentarios por parte del SC27, los cuales deberán finalizar en abril del 2007.

Su nombre completo es: "**Draft Text for ISO/IEC 3rd WD 27004**, Information Technology - Security tehcniques – Information Security Management Measurements".

- ISO/IEC: **ISO** (Organización Internacional de Estándares) e **IEC** (Comisión Internacional de Electrotécnia).
- **WD**: es la abreviatura de "Working Draft" (Borrador de trabajo).
- Information Security Management Measurements: Mediciones para la Gestión de la Seguridad de la Información.

  NOTA: Podría haberse traducido Management de otras formas, pero se optó por esta en asociación con **ISMS** y **SGSI:** Information Security Management System / Sistema de Gestión de la Seguridad de la Información.

A los efectos de este texto, esta norma será definida como:

"Borrador de trabajo ISO/IEC-27004: Mediciones para la Gestión de la Seguridad de la Información."

Como se hizo referencia en otros artículos, este futuro estándar no es algo aislado, sino que forma parte de la serie o familia **ISO-2700x** de los cuales se pueden considerar hoy:

- **ISO/IEC 27000** Fundamentals and vocabulary
- **ISO/IEC 27001 ISMS** - Requirements (revised BS 7799 Part 2:2005) – Publicado el 15 de octubre del 2005
- **ISO/IEC 27002** Code of practice for information security management - Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005
- **ISO/IEC 27003 ISMS** implementation guidance (bajo desarrollo)
- **ISO/IEC 27004** Information security management measurement (bajo desarrollo)
- **ISO/IEC 27005** Information security risk management (basado e incorporado a ISO/IEC 13335 MICTS Part 2) (bajo desarrollo)
- **ISO/IEC 27006** Requerimientos para organismos de acreditación (bajo desarrollo)

DESARROLLO

I. Introducción:

Como se mencionó en el prólogo, esta futura norma tiene como misión desarrollar todos los aspectos que deben ser considerados para poder "medir" el cumplimiento de la norma ISO 27001. Como ya se sabe, la misma hace especial hincapié en el concepto de SGSI y en la aplicación de controles, los cuales son los que en definitiva le dan vida a este ciclo permanente de gestión. El principio básico es que si no se puede medir, entonces no sirve de nada. Como se irá viendo a lo largo de este texto, la idea de medición es muy amplia y en definitiva, va desde la medición más simple hasta la combinación de varios niveles o instancias de ellas para poder ofrecer datos que lleven a un verdadero "cuadro de mando de la seguridad", que sería el objetivo último de todo el SGSI, y a través del cual, los diferentes niveles jerárquicos de la organización, podrán acceder a la información de seguridad, que a su nivel le hace falta conocer y en base a esta adoptar las decisiones correspondientes.

La norma ISO 27004, comienza con una Introducción, de la que se debe destacar:

> "El empleo de este estándar permitirá a las organizaciones dar respuesta a los interrogantes de cuán efectivo y eficiente es el SGSI y qué niveles de implementación y madurez han sido alcanzados. Estas mediciones permitirán comparar los logros obtenidos en seguridad de la información sobre períodos de tiempo en áreas de negocio similares de la organización y como parte de continuas mejoras".

El segundo apartado define el **ámbito**, como una guía sobre la especificación y uso de técnicas de medición, para proveer precisión en la observación del SGSI en cualquier tipo de organizaciones y con el **propósito** de crear una base para recolectar, analizar y comunicar datos relacionados a este SGSI, los cuales serán empleados para tomar decisiones que permitan mejorar el mismo.

Hace referencia a que es indispensable para la aplicación de este documento, el conocimiento del estándar ISO 27001:2005.

II. Terminología.

A continuación sólo se describen las definiciones fundamentales que serán empleadas en este texto.

Atributo: Propiedad o característica de una "entidad", que puede ser distinguida cuantitativa o cualitativamente, por una persona o sistema automatizado.

Entidad: Un objeto (tangible o intangible), que será caracterizado a través de la medición de sus "atributos".

Indicador: Es una medida que provee una estimación o evaluación de un "atributo" especificado, con respecto a las necesidades de información definidas.

III. Resumen del borrador de la norma ISO 27004.

1. Mediciones en un SGSGI:

Se basa sobre el modelo PDCA (Plan – Do – Check – Act) que es un ciclo continuo. Se podría resumir esto en la idea que, las mediciones están orientadas principalmente al "Do" (Implementación y operación de SGSI), como una entrada para el "Check" (Monitorizar y revisar), y de esta forma poder adoptar decisiones de mejora del SGSI a través del "Act"

Una organización debe describir como se interrelacionan e interactúan el **SGSI** y **las mediciones**, desarrollando guías que aseguren, aclaren y documenten esta relación, con todo el detalle posible.

Los objetivos de estos procesos de mediciones son:

- Evaluar la efectividad de la implementación de los controles de seguridad.
- Evaluar la eficiencia del SGSI, incluyendo continuas mejoras.
- Proveer estados de seguridad que guíen las revisiones del SGSI, facilitando mejoras a la seguridad y nuevas entradas para auditar.
- Comunicar valores de seguridad a la organización.
- Servir como entradas al plan de análisis y tratamiento de riesgos.

2. El modelo y método para las mediciones de seguridad:

Se debe desarrollar un programa de cómo ejecutar la medición de la seguridad de la información. El éxito de este programa, se basará en la asistencia o ayuda que estas mediciones aporten para adoptar decisiones, o determinar la eficiencia de los controles de seguridad. Por lo tanto este programa de mediciones debe estar basado en un "**Modelo**" de mediciones de seguridad de la información.

Este Modelo es una estructura que enlaza los *atributos* medibles con una *entidad* relevante. Estas entidades, incluyen procesos, productos, proyectos y recursos. Es decir, este modelo debe describir **cómo** estos atributos son cuantificados y convertidos a *indicadores* que provean bases para la toma de decisiones, sustentados en necesidades de información específica.

El primer paso para el desarrollo de este modelo, es definir los atributos que se consideran más relevantes para medir la información que se necesita. Un mismo atributo puede ser incorporado en múltiples mediciones, soportando diferentes necesidades de información.

Para definir **cómo** los atributos deben ser medidos, esta norma propone también un **Método**.

Existen dos tipos de métodos para cuantificar los atributos:

- Subjetivos: Implica el criterio humano.
- Objetivos: Se basan en una regla numérica, que puede ser aplicada por personas o recursos automatizados.

Los métodos de medición pueden abarcar varios tipos de actividades y un mismo método puede aplicar a múltiples atributos. Algunos ejemplos de métodos son:

- Encuestas/indagaciones.
- Observación.
- Cuestionarios.
- Valoración de conocimientos.
- Inspecciones.
- Re-ejecuciones.
- Consulta a sistemas.
- Monitorización (“Testing”)
- Muestreo.

Un tema a considerar es la asociación de mediciones con determinadas escalas, de las cuales se proponen los siguiente tipos:

- Nominal: Los valores son categóricos.
- Ordinal: Los valores son ordenados.
- Intervalos: Se poseen máximos y mínimos con distancias entre ellos.
- Ratio: Tienen escalas de distancias, relacionadas a mediciones.

La última referencia la hace respecto a la unidades de medición, recomendando emplear convenciones para uniformar las mismas

El último aspecto a considerar aquí es el de la **frecuencia**. Se deberían definir y programar claramente los intervalos en los cuales se llevará a cabo cada medición (Semanal, mensual, trimestral, anual, etc.). Considerando una relación entre la necesidad de contar con esta información y el esfuerzo para obtenerla (coste/beneficio).

3. Definición y selección de las mediciones en un SGSI:

La norma especifica también, como desarrollar las mediciones para poder cuantificar la eficiencia de un SGSI, sus procesos y controles.

La mediciones de la información pueden ser requeridas para:

- Gobierno Corporativo.
- Cumplimiento de regulaciones y/o requisitos legales.
- Operaciones o gestión organizacional.
- Certificación de un SGSI.
- Clientes, partners, socios de negocio, etc.
- Mejoras en la implementación y/o eficiencia del SGSI.
- Mejora de procesos.

Los pasos a seguir para el establecimiento y operación de un programa de mediciones son:

- Definición de los procesos
- El desarrollo de mediciones aplicables.
- La implementación del programa.
- Revisión de mediciones.

Finalmente todo el programa de mediciones debe ser revisado en pasos posteriores (y continuos), para verificar que el mismo sigue ofreciendo a la organización información válida, las fuentes y otros atributos continúan siendo correctos y los beneficios contra el esfuerzo requerido siguen siendo positivos. Como consecuencia de este análisis, las mediciones podrán ser mantenidas, eliminadas, sustituidas o modificadas.

Las mediciones están directamente relacionadas a:

- Procesos de sistemas de gestión (Ej: ¿Se realizaron las auditorías?, ¿Este manual cumple con los estándares?, etc.).
- Ejecución de controles de seguridad de la información (Ej: Volumen de incidencias por tipo, acceso a tablas, etc.).

Esta norma define dos categorías de mediciones:

- Mediciones de ejecución: Eficiencia.
- Mediciones de progreso: Cambios en la protección de la información.

Los constantes ciclos de estas mediciones requieren inicialmente un fase de **planeamiento**, donde se establezcan las premisas genéricas, se pueda elegir una selección de mediciones de información de seguridad y su categorización. Este planeamiento garantiza que el contexto de mediciones sea correctamente establecido. El planeamiento debe incluir identificación de recursos financieros, humanos y de infraestructura incluyendo los responsables de proveerlos y asignarlos para asegurar su correcta implementación.

Una medición para ser válida, debería cumplir con los siguientes criterios:

- Estratégico: Alineado con la estrategia y misión de seguridad de la información.
- Cuantitativo: Datos numéricos o empíricos, más que opiniones.

- Razonable: El valor del dato recolectado no debería ser mayor al coste de recolectarlo.
- Verificable: Cualquier revisión por parte de un tercero, debería ser capaz de valorar el dato y obtener resultados.
- Tendencia: Los datos deberían ser representativos del impacto, cada vez que se imponen cambios.
- Usable: Los resultados deberían apoyar la toma de decisiones.
- Indivisible: Los datos deberían ser recolectados al más bajo nivel de desagregación posible.
- Bien definido: Bien documentadas sus características como frecuencia, fórmula, evidencia e indicadores.

Para seleccionar los controles adecuados, las organizaciones deberían realizar los siguientes pasos:

- Definir un programa (como se mencionó en los puntos anteriores).
- Seleccionar los objetivos de control y los controles a ser incluidos en las mediciones.
- Definir los indicadores para los controles seleccionados.

Las mediciones seleccionadas deberían reflejar la prioridad de la información que se necesita, las mismas deben ser documentadas. Ejemplos de ellas las presenta en el ANEXO A de la norma.

Se presentan a continuación campos que pueden contemplar:

- Nombre.
- Propósito.
- Tipo de propósito.
- Ámbito o dominio.
- Método de medición.
- Escala.
- Roles.
- Método de recolección de datos.
- Ciclo de vida.
- Criterio.
- Campos del indicador: Efectos de impacto, causas de desvío, gráficas.

La organización debe documentar su plan para la implementación de las mediciones de seguridad de la información y llevar adelante el mismo. Esta implementación podría contemplar:

- Listado de mediciones a ser recolectadas y empleadas, incluyendo sus especificaciones.
- Definición de pasos para recolección y análisis de los datos medidos.
- Identificación de formatos de reporte para cada medición.
- Definir un ciclo de refresco de las mediciones para asegurar su corrección en relación al SGSI.

4. Operación de las mediciones del SGSI (Fase DO: Hacer)

Las mediciones deben encontrarse totalmente integradas al SGSI incluyendo:

- Definición y documentación de roles y responsabilidades que participan en el desarrollo, implementación y mantenimiento de las mediciones dentro del contexto del SGSI.
- Políticas y procedimientos que definan el empleo de las mediciones en la organización, difusión de la información medida, auditoría y revisión de los procesos de medición.
- Procesos de monitorización de las mediciones para evaluar su uso.
- Procesos de eliminación, modificación y adición de nuevas mediciones, para asegurar que las mismas envuelven a toda la organización.

La fase "Do" es una de las que establece el enlace entre las mediciones que resultan adecuadas para cubrir en la organización en un momento dado. Durante esta fase, los resultados del programa de mediciones debería ser revisado y aprobado. En este momento se decidirán los recursos que se asignarán para la implementación de las mediciones. La Dirección deberá acordar este conjunto de mediciones planificadas , para lanzar las tareas con los recursos y la infraestructura correspondiente.

5. Mejoras de las mediciones del SGSI (Fases Check y Act: monitorizar/auditar y actuar).

Las fases "Check" y "Act" facilitarán las mejoras y reencauces de los procesos de medición, y permitirán el análisis de la información de mediciones disponibles y su apoyo para la toma de decisiones. En todo este ciclo, las mediciones deberán ser evaluadas, ajustadas y detectadas a las necesidades del SGSI, asegurando que su evolución continúe cubriendo los objetivos de seguridad, respecto a la posición de partida del proceso.

Se debería identificar la frecuencia de estas fases, y en estos períodos realizar las revisiones y establecer los mecanismos para hacer posible la reactivación o el lanzamiento automático de fases de revisión para detectar los desvíos de las condiciones iniciales.

Este punto presenta dos aspectos:

1) Definir un criterio para evaluar la información (Análisis de información).
2) Definir un criterio para evaluar el proceso de mediciones (Validación de mediciones).

Las mediciones deberían ser revisadas, cuando ocurran cambios en la organización. Para asegurar que las mediciones reflejan el estado actual de seguridad, es importante verificar que los datos siguen siendo válidos. Las revisiones se deben realizar también a intervalos planeados, para verificar si se siguen ejecutando tal cual se diseñó en su momento. También se recomienda la realización de evaluaciones externas para proveer una visión independiente del programa.

El propósito de estas revisiones es asegurar que:

- Las mediciones son correctamente revisadas al ocurrir cambios en los objetivos de negocio.
- Las mediciones que no se suelen emplear son quitadas e ingresan nuevas mediciones necesarias.
- Los recursos que soportan estas mediciones son los adecuados.
- Las decisiones sean documentadas para permitir futuras comparaciones, o analizar tendencias.

Los resultados de estas mediciones deberían ser difundidos a todo el personal interesado, directivos, gerentes, técnicos y personal relacionado a la seguridad. El formato de estos reportes debe ser acorde a las necesidades de cada grupo o perfil al que va dirigido e informar los aspectos que cada uno necesita, con el grado de detalle adecuado a su función o rol en la organización.

Algunos ejemplos de reportes se presentan en el ANEXO A de la norma. Se debe considerar la confección de reportes internos y externos a la organización con las restricciones pertinentes en cada caso, controlando y auditando con máxima precaución lo que se difundirá externamente.

Es muy importante que estos reportes faciliten la "realimentación" de información, basada en lo que puedan aportar sus consumidores, y generar los mecanismos necesarios para analizar e implementar este ciclo de retorno.

6. La dirección.

La Dirección debería establecer y mantener acuerdos en sus mediciones. Su implementación debe ser acorde a lo que establecen los estándares internacionales, teniendo en cuenta la aceptación de los requerimientos de mediciones.

- Deberán establecerse acuerdos entre la Dirección y el personal que llevará adelante esta tarea de mediciones. Demostrando el interés de todos los niveles de la organización, por ejemplo a través de mediciones en la política de seguridad, asignación de responsabilidades, servicios, preparación, presupuesto y recursos.
- Todos los acuerdos deberían ser comunicados a la organización.

La Dirección deberá proveer evidencias de estos acuerdos, de su implementación, operación, revisión, monitorización, mantenimiento y mejora de todo el programa de mediciones a través de:

- Establecimiento del programa de mediciones.
- Asegurar que el programa sea implementado.
- Establecer roles y responsabilidades en el programa de mediciones.
- Comunicar a todo el personal interviniente el programa de mediciones y sus indicadores de progreso.
- Proveer suficientes recursos para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el programa de mediciones.
- Asegurar que las auditorías internas del programa de mediciones, como una parte de las auditorías SGSI, sean las correctas.
- Las revisiones del programa de mediciones sean parte del SGSI

La dirección deberá asignar y proveer los recursos para el programa de mediciones, incluyendo los responsables de todos los aspectos y la infraestructura para llevar adelante sus funciones.

La dirección deberá asignar los siguientes roles y responsabilidades para la ejecución y uso de las mediciones:

- Propietario de la medición.
- Persona o unidad responsable del requerimiento de mediciones.
- Persona o unidad responsable de recolectar y almacenar los atributos de información de una entidad objeto de medición.
- Persona o unidad responsable de la comunicación a la organización, de la importancia del programa de mediciones y sus resultados, para asegurar su aceptación y empleo.

- Persona o unidad responsable de la evaluación del programa de mediciones, para asegurar que se corresponde con los controles de seguridad.
- Personas que intervienen y dirigen el programa de mediciones.

Será necesario establecer autorizaciones, certificaciones y/o acreditaciones al personal que llevará a cabo estas tareas y los criterios para la formación técnica de los mismos, como así también la capacitación de todo el personal interviniente, respecto a los temas fundamentales que envuelve el proceso de mediciones.

La dirección deberá asegurar que todo el personal sea conciente de lo relevante e importante que es el programa de mediciones y como cada uno de ellos contribuyen a mejorar estos objetivos de

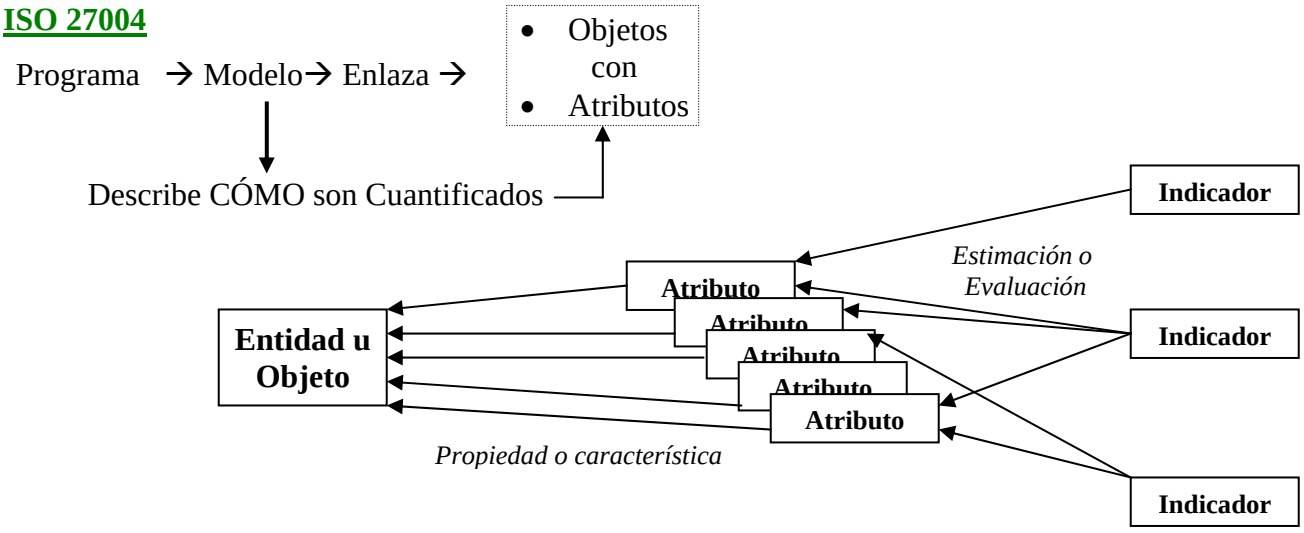
SGSI.

IV. Conclusiones finales.

En este texto, se trató fundamentalmente de demostrar que es importante "Medir el SGSI", y de hacerlo, esta norma propone un lenguaje común que permite seguir avanzando de la mano de la normalización.

Tal vez lo más importante es que una vez más hace presente la idea de ciclo, pues estas mediciones también se llevan a cabo de esta forma, y justamente por ser así es que facilitan la concreción de un verdadero cuadro de mando "Vivo" que ofrece la información que necesita cada nivel de la empresa.

Deseo cerrar este texto presentando en forma esquemática lo que se puede llevar a cabo a través de la **combinación de ISO 27001 e ISO 27004.** Desde la definición de los controles, requerimientos, atributos e indicadores, para llegar finalmente a los niveles de agrupamiento/desagregación de información que más se desee.



ISO 27001

ISO 27004

EJEMPLO:
ISO 27001
Punto **A.11**
(Control
de accesos)

Ctrl	Nombre
[01]	Política de Control de Accesos
[02]	Registro de usuarios
[03]	Administración de privilegios
[04]	Administración de contraseñas de usuario
[05]	Revisión de derechos de acceso de usuarios
[06]	Equipamiento de usuario no atendido
[07]	Política de limpieza de escritorio y pantallas
[08]	Política de uso de los servicios de red
[09]	Autenticación de usuarios para conexiones externas
[10]	Identificación de equipamiento de redes
[11]	Protección de configuración y diagnóstico de puertos
[12]	……
[“n”]	……

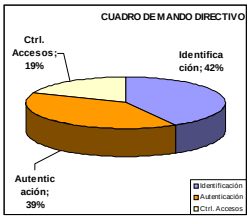
Requisitos
Requisitos
Requisitos
Requisitos
Requisitos

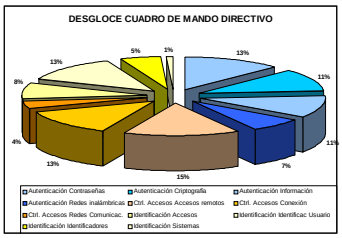
Atributo
Atributo
Atributo
Atributo
Atributo

Indicadores
Indicadores
Indicadores
Indicadores
Indicadores

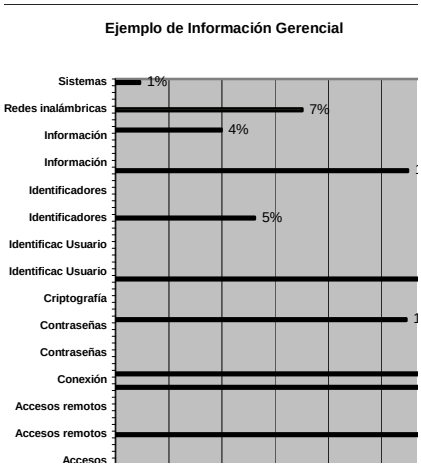
Cuadros de mando

Información Directiva





Información Gerencial



Información Técnica

Indicador	Agrupación	Valor IDEAL	Peso min:1 Máx:10	%cumplim. EJEMPLO
% Sistemas con prohibición de Acceso anónimo	Accesos	100	8	10%
% Sistemas que tienen implementado registros de accesos erróneos	Accesos	100	6	12%
% Sistemas que tienen implementado registros de accesos correctos	Accesos	100	4	13%
% Sistemas que tienen implementado registros de accesos	Accesos	100	5	16%
% de sistemas que implementan perfiles de acceso	Accesos	100	5	75%
% de sistemas que implementan perfiles de acceso y presentan opciones a los usuarios en función de su perfil	Accesos	100	5	33%
% de sistemas específicos de control de acceso	Accesos	indiferente	1	43%
% de sistemas específicos de control de acceso que poseen mecanismos robustos para esta actividad	Accesos	100	8	27%
% de sistemas específicos para el control de accesos remotos	Accesos remotos	indiferente	1	81%
% de sistemas específicos para el control de accesos remotos que implementan registros de accesos localmente	Accesos remotos	0	5	23%
% de sistemas específicos para el control de accesos remotos que implementan registros de accesos de forma centralizada	Accesos remotos	100	7	45%
% de sistemas específicos para el control de accesos remotos que implementan registros de actividad realizada.	Accesos remotos	100	8	66%
% de sistemas específicos para el control de accesos remotos que implementan Certificados digitales	Accesos remotos	100	8	53%
% de accesos remotos por proveedor	Accesos remotos	indiferente	1	12%
% proveedores que acceden remotamente y poseen acuerdos de confidencialidad	Accesos remotos	100	7	23%
% de sistemas que limitan el tiempo de conexión	Conexión	100	4	45%
% de sistemas críticos que limitan el tiempo de conexión	Conexión	100	10	67%
% Sistemas que poseen mecanismos de generación aleatoria de contraseñas	Contraseñas	100	6	8%
% Sistemas que fuerzan el cambio de contraseñas	Contraseñas	100	9	65%
% de contraseñas iniciales cambiadas	Contraseñas	100	9	43%
% Sistemas que separan los canales de notificación de usuario y contraseña	Contraseñas	100	10	23%
% Sistemas que premiten el cambio de contraseña.	Contraseñas	100	5	59%
% Sistemas que disponen histórico de contraseñas.	Contraseñas	100	4	18%
% Sistemas que cumplen con la sintaxis de contraseñas	Contraseñas	100	7	62%
% Sistemas que guardan cifradas las contraseñas	Contraseñas	100	10	22%
% Sistemas que cifran la información de autenticación en la transmisión	Criptografía	100	10	36%
% de usuarios con Certificados digitales	Criptografía	100	6	75%
% de terceros que poseen acuerdo criptográficos con Telefónica	Criptografía	100	7	43%
% de sistemas que almacenan Claves privadas de Certificados Digitales	Criptografía	indiferente	1	33%
% de sistemas que comprueban validez y caducidad de Certificados Digitales	Criptografía	100	6	44%
% de terceros que poseen certificados digitales	Criptografía	100	5	57%
% Sistemas que utilizan autenticación robusta	Identificac Usuario	100	9	12%
% Sist que tienen mecanismos de IA	Identificac Usuario	100	10	34%
% Identificadores genéricos con responsable	Identificac Usuario	100	8	77%

Alejandro Corletti Estrada - Madrid, marzo de 2007.