Marco de Referencia para la Clasificación de Bienes Intangibles de la Corporación CENACE Aplicando la Norma ISO 27000

M. Chanatasig

Corporación Centro Nacional de Control de Energía - CENACE

Resumen **- Uno de los principales bienes intangibles de la corporación CENACE es la información que se genera a través de sus procesos de negocio. Su alineación con las estrategias corporativas generan un valor agregado de gran importancia por su participación en el desarrollo económico del país. Teniendo esto presente es necesario brindarle especial atención al tema de seguridad de la información Corporativa.**

El presente trabajo pretende proponer un marco de referencia que permita al CENACE disponer de lineamientos generales para el análisis y clasificación de la información de la Corporación, de acuerdo con las políticas definidas previamente a través del REGLAMENTO INTERNO DE USO, ADMINISTRACIÓN Y CONFIDENCIALIDAD DE LA INFORMACIÓN Y DE LOS RECURSOS Y SISTEMAS INFORMÁTICOS DE LA CORPORACIÓN CENTRO NACIONAL DE CONTROL DE ENERGÍA – CENACE, aprobado en el año 2008 y de conformidad con lo estipulado en la norma ISO 27000, con el propósito de proteger la información sensible y crítica soportada por los sistemas de información de CENACE.

1. INTRODUCCIÓN

El conocimiento o información generada a través del trabajo intelectual de los individuos, ha sido reconocido como un bien o activo intangible, cuyo valor llega a ser equiparable o en ciertos casos de mayor importancia que los bienes tangibles que disponen las organizaciones.

En el caso de la Corporación CENACE, su información es un activo organizacional esencial y vital para la ejecución de sus procesos de negocio, los cuales finalmente generan un aporte fundamental y directo en el desarrollo económico del Ecuador.

Dado este grado de importancia, los activos intangibles de CENACE requieren disponer de los niveles de protección apropiados que permitan garantizar su disponibilidad, confidencialidad e integridad, es decir que cuenten con un nivel de seguridad adecuado.

En este ámbito, se requiere disponer de un marco referencial para ejecutar la clasificación de la información de la Corporación CENACE y se ha considerado apropiado el aplicar un estándar, como la norma ISO 27000, la cual contiene los lineamientos para que las empresas puedan lograr y mantener una apropiada protección para sus activos o bienes intangibles organizacionales. Todo esto en concordancia con las políticas de seguridad corporativas.

2. ACTIVOS INTANGIBLES

Por definición, un activo es todo lo que tenga valor para la organización (ISO/IEC 13335-1:2004).

En este contexto, es muy común que al interior de las empresas se manejen los términos "activos tangibles" y "activos intangibles". El primero se refiere a todos aquellos bienes de naturaleza material que se puede tocar y por consecuencia lo segundo se constituye como todos aquellos bienes de naturaleza inmaterial que no se pueden tocar, conocido también como capital intelectual.

Sin embargo, algunos autores resaltan que ambos tipos de bienes coexisten juntos y deben ser fusionados para que la organización pueda funcionar.

Thomas Steward en [1], define al capital intelectual como *"material intelectual, conocimientos, información, propiedad intelectual, experiencia, que puede utilizarse para crear valor*".

Una clasificación que se le puede dar a este concepto relativamente nuevo, es aquella propuesta en Wikipedia como sigue a continuación:

1. **Capital humano:** Se trata de las capacidades, actitudes, destrezas y conocimientos que cada miembro de la empresa aporta a ésta (Know How).

2. **Capital organizacional:** Se incluyen todos aquellos elementos de tipo organizativo interno que pone en práctica la empresa para desempeñar sus funciones de la manera más óptima posible.

Entre estos se pueden señalar las bases de datos, los cuadros de organización, los manuales de procesos, la propiedad individual (patentes, marcas o cualquier elemento intangible que pueda estar protegido por los derechos de propiedad intelectual) y todas aquellas cosas cuyo valor para la empresa sea superior al valor material.

3. **Capital relacional:** Hace referencia a los posibles clientes a los que va dirigido el producto de una empresa, a los clientes fijos de ésta (cartera de clientes, listas establecidas, etc.), y a la relación empresa-cliente (acuerdos, alianzas, etc.); y también a los procesos de organización, producción y comercialización del producto (estrategias de cara al logro).

3. GESTIÓN DE ACTIVOS

Un elemento esencial para la clasificación de la información es lo que tiene que ver con la gestión de activos, esto incluye a los activos intangibles o capital intelectual, que dispone una organización.

En el ámbito de este estudio, el activo esencial es la información o datos que maneja la organización y alrededor de estos se pueden identificar otros activos importantes.

Serrano, en [3], dice que la Gestión de Información, puede ser entendida genéricamente como las actividades orientadas a controlar, almacenar y recuperar la información que posee una organización.

Así, se puede entender por gestión de la información como un proceso que incluye operaciones como extracción, manipulación, tratamiento, depuración, conservación, acceso y/o colaboración de la información adquirida por una organización a través de diferentes fuentes y que gestiona el acceso y los derechos de los usuarios sobre la misma.

También son parte de las actividades de la gestión de información la definición de estrategias, planes, políticas, procedimientos, controles, y mejora continua para el tratamiento de la información.

3.1. Inventario de Activos

3.1.1. Auditoría de Información

Serrano, en [3], menciona que, "*no será posible desarrollar una buena estrategia de gestión de la información sin analizar previamente la información que posee la organización o, lo que es lo mismo, auditar la información*".

Serrano, en [3], indica que, una auditoría de información es un proceso que permite detectar, controlar y evaluar la información que existe en una organización y los flujos de información que en ésta discurren, el uso que se hace de ella y su adecuación con las necesidades de su personal y con los objetivos de la organización.

De acuerdo a Serrano, en [3], existen diferentes metodologías para realizar las auditorías de la información. A nivel general recomienda observar las siguientes fases:

1. Planificación. Desarrollar de forma clara los objetivos, saber qué queremos conseguir, conocer la organización e identificar a las personas claves en la organización (no a nivel jerárquico, sino funcional). Conocer la envergadura del proyecto y los recursos (envergadura física, de información, humanos, financieros y de localización de recursos). Escoger la metodología: colección, análisis y evaluación de datos, presentación de finalidades y recomendaciones y plan de acción para su implementación. Desarrollar un plan estratégico y de comunicación: antes, durante y después de la auditoría. Alistar la gestión del soporte, desarrollar un plan de negocio, encontrar una forma de fomentar o promover.

2 Colección de datos. Desarrollar una base de datos de recursos de información. Preparación para la colección de datos, cuestionario, entrevistas en grupo e individuales.

3 Análisis y preparación de los datos, métodos de análisis.

4. Evaluación de datos, evaluar vacíos y duplicaciones, interpretar el flujo de información, evaluar los problemas, formular recomendaciones, desarrollar un plan de acción para el cambio.

5 Comunicar recomendaciones, escribir el informe, presentaciones orales y seminarios, intranets/ extranets corporativos, obtener feedback con participantes y personas claves en el proceso.

6 Implementación de las recomendaciones. Desarrollar un programa de implementación, incorporar los cambios dentro de los planes formales (marketing, negocios y estrategia), desarrollar una estrategia de post-implementación, desarrollar una política de información.

7. Continuar con el seguimiento de la auditoría. Medir y valorar los cambios, planear un ciclo de auditoría de información regular.

Lo antes indicado, coincide con los lineamientos de la norma ISO 27001 y 27002, en [4] y [5] donde se hace referencia al levantamiento del inventario de activos como parte de la Gestión de Activos.

Esto lleva a colegir que CENACE podría acoger la recomendación de ejecutar una auditoría de información con miras a para lograr una gestión de información y consecuentemente una clasificación de información adecuada.

3.1.2. Levantamiento de Inventario de Activos

Como se menciono con anterioridad, el activo esencial es la información o datos que maneja la organización y alrededor de estos se pueden identificar otros activos relevantes como los siguientes:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

A continuación se propone los pasos a ejecutar para la preparación del inventario de activos:

- Identificación de activos (dentro de los tipos definidos en [6]).
- Relaciones de dependencia.
- Valoración.

Fase 1: Identificación de Activos

Por cada activo se obtendrá la siguiente tabla:

Tabla 1: Formato para identificación de activos

[X] Tipo de Activo	
Código: XXX	Nombre: XXXXX
Descripción: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
Propietario: XXXXXXXXXXX	
Responsable: XXXXXXXXXX	
Otros datos relevantes del activo:	

Donde:

• Tipo de Activo:
- [S] Servicios
- [D] Datos / Información
- [SW] Aplicaciones (software)
- [HW] Equipos informáticos (hardware)
- [COM] Redes de comunicaciones
- [SI] Soportes de información
- [AUX] Equipamiento auxiliar
- [L] Instalaciones
- [P] Personal

Fase 2: Relaciones de Dependencia

Los activos más llamativos suelen ser los datos y los servicios; pero estos activos dependen de otros activos más triviales como pueden ser los equipos, las comunicaciones o las frecuentemente olvidadas personas que trabajan con aquellos. Por ello aparece como importante el concepto de "dependencias entre activos" o la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

En la tabla de cada activo añadiremos una fila por cada activo dependiente [hijos] y clasificaremos el grado de dependencia como: Bajo, Medio y Alto.

Tabla 2: Formato para definir relaciones de dependencia

Nombre Activo [padre]	
Dependencias de activos inferiores [hijos]	Grado de Dependencia
Activo hijo1	
Activo hijo2	
……..	
Activo hijoN	

Fase 3: Valoración:

Dos formatos:

1. Por cada activo añadir los siguientes campos a la tabla:

Tabla 3: Formato para definir valoración (formato 1)

Valoración		
Dimensión	Valor	justificación
[X]		
[X]		
[X]		

2. Tabla de activos / Dimensiones de valoración:

Tabla 4: Formato para definir valoración (formato 2)

Activos	[D]	[I]	[C]
Activo1	*Valor1-D*	*Valor1-I*	*Valor1-C*
Activo2	*Valor2-D*	*Valor2-I*	*Valor2-C*
…..	……	…..	…..
ActivoN	*ValorN-D*	*ValorN-I*	*ValorN-C*

Donde:

• Dimensión:
- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos

• Valor:

Tabla 5: Tabla de Valores

Valor		Criterio
10	Muy alto	Daño muy grave a la organización
7-9	Alto	Daño grave a la organización
4-6	Medio	Daño importante a la organización
1-3	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Otros elementos a tener en cuenta dentro del proceso de levantamiento de inventario son los siguientes:

Criterios: Al momento de levantar su inventario, el propietario podría aplicar los siguientes criterios:

- Identificar información necesaria, útil y actualizada para incluirla en el inventario.
- Información no útil y desactualizada separarla y desecharla del inventario.
- Información que no pertenece al usuario o que puede ser de utilidad para otro usuario debe ser transferida a quien corresponda y no incluir en el inventario para que sea tratada por el usuario que se haga responsable.

3.2. Propiedad y Responsabilidad sobre los Activos

Una vez levantado el inventario, la organización oficialmente ratificará o rectificará los propietarios sobre la información identificada.

También es pertinente que la organización defina un comité de gestión de información cuyos integrantes deberán ser funcionarios de nivel ejecutivo. En el caso de CENACE podría ser el mismo Comité Ejecutivo.

Adicionalmente, se deberá definir oficialmente las responsabilidades para los propietarios y miembros del comité de gestión de información.

Parte de las responsabilidades del comité de gestión de información son la definición de estrategias y políticas y reglamentos de gestión como por ejemplo la definición del ciclo de vida de la información, reglas para el uso de información (correo electrónico, dispositivos móviles, etc.).

Algunas de las responsabilidades que tienen los propietarios son las siguientes:

Inventario: Ejecutar el levantamiento de inventario de información y revisar su validez y restricciones de acceso, dar de alta o de baja un elemento de inventario, con la frecuencia que indiquen las políticas o procedimientos definidos.

Documentación: Definir, mantener o actualizar los procedimientos (gestión de activos, gestión de conocimiento, levantamiento de inventarios, etiquetas de activos, etc.).

3.3. Clasificación de la información

Según el estándar MAGERIT, en [6], la Información Clasificada es aquella sometida a normativa específica de control de acceso y distribución; es decir aquella cuya confidencialidad es especialmente relevante. La tipificación de qué información debe ser clasificada y cuales son las normas para su tratamiento, vienen determinadas por regulaciones sectoriales, por acuerdos entre organizaciones o por normativa interna de la empresa.

Para la ejecución de la clasificación de la información se debe contar con el inventario de información que dispone la Corporación.

Un elemento adicional es la definición de los niveles de clasificación de información, para lo cual se ha escogido el estándar MAGERIT indicado en [6]. A continuación se presentan los niveles de clasificación de información según el estándar referido:

- [S] secreto
- [R] reservado
- [C] confidencial

- [DL] difusión limitada
- [SC] sin clasificar

Una vez que hemos decidido, cuál será la clasificación de nuestra información, en conjunto con el "propietario" de la información se desarrollará el criterio, para saber a cuál de las diferentes clasificaciones pertenece la información. Para poder determinar la sensibilidad de la información se tendrá que tomar en cuenta los siguientes criterios:

- Uso de la información.
- Valor de la información.
- Edad de la información.
- El nivel de daño que podría causar la información, si ésta es revelada o robada.
- El nivel de daño que podría causar la información, si es alterada o está corrupta.
- Protección de datos, ante autoridades, como leyes, regulaciones o nivel de responsabilidad del empleado, dentro de la empresa.
- Efectos de que la información sea de seguridad nacional.
- ¿Quién deberá tener permisos de acceso a la información?
- ¿Quién deberá darle mantenimiento a la información?
- ¿En donde deberá resguardarse esta información?
- ¿Quién deberá tener la responsabilidad de reproducir la información?
- ¿Qué información requiere de una etiqueta y marca especial?

Estas son varias de las tareas que se deberá hacer, antes de efectuar la clasificación de la información, una vez clasificada la información se tendrá que seguir un Procedimiento de Clasificación de la Información, a fin de que cada vez que se tenga información de nuevos proyectos, se sepa desde un principio como clasificar la información, a continuación se proponen los pasos a seguir, para tener un procedimiento de clasificación:

1. Identificar al propietario de la información, quien a su vez, será el responsable del mantenimiento de datos y el nivel de seguridad de su información.

2. Especificar los criterios que determinarán, como se clasificará la información.

3. El propietario de los datos deberá indicar la clasificación de la información y será el responsable de esta tarea.

4. Indicar los niveles de control que se requieren, para cada nivel de clasificación.

5. Documentar todos los problemas y excepciones que se tuvieron, previos a la clasificación.

6. Indicar la metodología a seguir, cuando se tenga que transferir la custodia de los datos a diferentes propietarios de la información.

7. Indicar cuál será el procedimiento, para desclasificar la información, una vez que ya no aplique.

8. Integrar esta enseñanza en el programa de capacitación a nuevos empleados de la organización, para que aprenda a manejar el uso de la clasificación de la información en sus diferentes niveles de seguridad.

Otros elementos a tener en cuenta dentro del proceso de clasificación son los siguientes:

Herramientas: Para el levantamiento y gestión del de información de debe disponer de un sistema informático. Este permitirá registrar las características de la información como son: tipo, formato, ubicación, propietario, nivel de protección, etc., de acuerdo con lo especificado en [5] sección 7.1.1 Inventario de Activos.

Políticas: La organización deberá evaluar la actual política de seguridad de CENACE, principalmente artículos 16 al 26 y proponer la complementación que corresponda.

4. CONCLUSIONES Y RECOMENDACIONES

1. Para la ejecución exitosa de una clasificación de información es requisito disponer de un adecuado inventario de información corporativa. Para disponer del inventario inicial se hace necesaria la ejecución de una auditoria de información al menos en un inicio.

2. Se sugiere evaluar la complementación de la Política de Seguridad Corporativa de CENACE, según corresponda, en caso de acoger alguna de las recomendaciones planteadas en este artículo.

3. La clasificación de información se muestra como una tarea de gran tamaño motivo por el cual sería recomendable que esta se ejecute a través de un proyecto de Gestión de Información con el soporte externo de una empresa especializada en el tema.

4. El presente artículo requiere ser complementado para que a futuro se pueda constituir en un marco de referencia ajustado a la realidad del CENACE.

AGRADECIMIENTOS

Agradezco a mi esposa Sandrita por brindarme su apoyo para poder realizar este trabajo. Sin la ayuda de ella no hubiese sido posible la consecución de este artículo. El sacrificio que ella realiza por todos los miembros de la familia es digno de resaltar y homenajear.

REFERENCIAS BIBLIOGRÁFICAS

[1] Stewart T. (1997), *El Capital Intelectual: La nueva riqueza de las organizaciones*, Ediciones Granica S.A., Buenos Aires, Argentina.

[2] http://www.gestiondelconocimiento.com/conceptos_capitalintelectual.htm

[3] Serrano S. & Zapata M., "Gestión del Conocimiento: Auditar la Información para Gestionar el Conocimiento". Disponible (on line) en: http://www.gestiondelconocimiento.com/pdf-art-gc/00329sserrano.pdf

[4] ISO/IEC 27001 (2005), *Tecnología de Información-Técnicas de Seguridad-Sistemas de Gestión de Seguridad de la Información-Requerimientos*.

[5] ISO/IEC 27002 (2005), *Tecnología de Información-Técnicas de Seguridad-Código de Practica para la Gestión de Seguridad de la Información*.

[6] MINISTERIO DE ADMINISTRACIONES PÚBLICAS (2006), Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información-MAGERIT versión 2-Catálogo de Elementos. Madrid, España.

Marco O. Chanatasig V.- Nació en Pifo en el año 1971. Recibió su título de Ingeniero de Sistemas de Computación e Informática de la Escuela Politécnica Nacional de Quito en el 2000; y su título de Diplomado de Gestión de Servicios de la Tecnología de Información en el Tecnológico de Monterrey en 2008. Sus áreas de investigación están en el ámbito de la Gestión de Tecnologías de Información.