MODELO DE CLASIFICACIÓN DE ACTIVOS PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

VIVIANA VELANDIA MORALES

UNIVERSIDAD PILOTO DE COLOMBIA

ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA

ÁREA DE GESTIÓN DE LA SEGURIDAD Y EL RIESGO

BOGOTÁ D.C.

2013

MODELO DE CLASIFICACIÓN DE ACTIVOS PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

VIVIANA VELANDIA MORALES

Trabajo de investigación para optar por el título de Especialista en Seguridad Informática

Asesor

Richard García Rondón

MSc. Sistemas y computación

UNIVERSIDAD PILOTO DE COLOMBIA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

ÁREA DE GESTIÓN DE LA SEGURIDAD Y EL RIESGO

BOGOTÁ D.C.

2013

Nota de aceptación:

_____
_____
_____
_____
_____
_____

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá D.C. 28 de Febrero de 2013

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACTIVO: cualquier cosa que tenga valor para la organización

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

IMPACTO: cambio adverso en el nivel de los objetivos del negocio logrados.

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos

RIESGO: potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

SGSI: sistema de gestión de seguridad de la información

RESUMEN

La Organización para la Cooperación y el Desarrollo Económico, en su sesión 1037 de 25 de julio de 2002 estableció las Directrices para la Seguridad de los Sistemas y Redes de Información debido al entorno tecnológico que están adoptando los gobiernos, las empresas y las organizaciones para el manejo y administración de su información.

Los dispositivos que integran la infraestructura de acceso a la información se ha multiplicado lo que ha facilitado su intercambio y disposición. Este hecho está exponiendo la información a variedades de amenazas que son importantes identificar para garantizar su protección.

El modelo desarrollado establece una guía para que sean identificados todos los elementos que permiten el intercambio y acceso a la información, denominados ACTIVOS, tipificándolos según su naturaleza y propósito, para que según estas características, sean identificados los niveles de confidencialidad, integridad y disponibilidad para evitar pérdidas económicas, incumplimientos regulatorios y fallos en la operación.

La ventaja del modelo es que permite reflejar la relevancia que tiene para la organización verse afectado en aspectos referentes a la operación, la economía y el cumplimiento según su objeto de negocio, obteniendo los niveles requeridos en la confidencialidad, integridad y disponibilidad de los activos, para mantener la información protegida, completa y asequible.

La definición de la metodología se hizo en base a la Norma ISO 27001

Palabras clave: Clasificación de Activos, Seguridad de la información, ISO 27001, Sistema de gestión de seguridad de la información, SGSI, Dimensiones de seguridad de la información.

INTRODUCCIÓN

En el contexto empresarial el manejo de los datos y en general de la información, debe ser controlado con el fin de brindar protección a los individuos, a la propiedad intelectual, a los desarrollos y al conocimiento generado al interior de una organización.

La Organización Internacional para la Estandarización ha publicado la Norma ISO 27001:2005[1] que establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información, que tiene como fin el tratamiento de los riesgos de seguridad a los que se enfrentan las organizaciones por el uso de la información y de los sistemas que la soportan.

Esta norma establece diferentes controles que se deben tener en cuenta cómo la identificación de la responsabilidad de los activos y su clasificación, según su sensibilidad, criticidad e impacto.

La clasificación de los activos permite identificar los niveles de confidencialidad, integridad y disponibilidad de la información según el impacto que puede generar su divulgación, acceso no autorizado, modificación indebida o su no disponibilidad, sobre diferentes aspectos organizacionales cómo la operación, la economía y el cumplimiento, dándole mayor relevancia a aquellos activos que afecten aspectos o propiedades que sean establecidos de mayor interés.

Por medio de la implementación del modelo se podrán gestionar y garantizar los principios mínimos de seguridad dando cumplimiento a las nociones primitivas de seguridad del manejo de un sistema de información y su información.

[1] INTERNATIONAL STANDARD ORGANIZATION. Information technology -Security techniques - Information security management systems -Requirements. ISO/IEC 27001:2005. 1 ed. Geneve, Suiza: ISO, 2005.

1 DEFINICIÓN DEL PROBLEMA

Cuando una organización desea asegurar la información del negocio se encuentra con el siguiente problema: ¿Cuál es la información que debe proteger y cómo identificarla de forma apropiada?

La información está distribuida en diferentes tipos de sistemas que facilitan la interacción entre esta y los usuarios por lo que es fundamental que sean identificados todos los sistemas y activos que constituyen el flujo de la información dentro de los procesos de la organización, para que sean clasificados según su valor e importancia y así gestionar adecuadamente los riesgos a los que puede estar expuesta la información del negocio.

Implementar un método de clasificación que permita reconocer los activos que soportan la información y las afectaciones que podría causar al negocio la degradación de sus propiedades, facilita el mantenimiento de la seguridad y hace más efectiva la gestión de los riesgos.

El modelo de clasificación planteado establece una guía para identificar la información y los activos que la soportan, catalogándolos en diferentes tipos según su naturaleza y propósito, para que a partir de estas características se determine como se deben valorar sus principios y se identifiquen los niveles de impacto que causarían a la organización, según su implicación en el objeto del cumplimiento de la misión del negocio.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Desarrollar un modelo de clasificación de activos cumpliendo con los requerimientos mínimos establecidos para la implementación de un Sistema de Gestión de seguridad de la información que valore consistentemente las propiedades de seguridad de la información sobre cada uno de ellos y los clasifique dependiendo del impacto que puedan generar a la organización reflejando su valor e importancia.

2.2 OBJETIVOS ESPECÍFICOS

- Definir cuáles son los diferentes tipos de activos que deben relacionarse en un Sistema de Gestión de seguridad.
- Establecer una escala de medición de los activos que diferencie el nivel de impacto que puede generar a la organización en su operación, economía o cumplimiento y el nivel de clasificación que debe tener en su confidencialidad, integridad y disponibilidad.
- Guiar en cómo se debe evaluar los principios de seguridad de la información según el tipo de activo identificado.

2.3 HIPÓTESIS DE INVESTIGACIÓN

H_i: Para definir un método de clasificación adecuado para la gestión de la seguridad de la información de una organización y los activos que la soportan, es necesario tener en cuenta que la afectación de las propiedades de la información generará un impacto al negocio y el grado de este impacto dependerá así mismo del tipo de activo que se esté evaluando y de la propiedad que se haya visto comprometida.

3 MARCO TEÓRICO

3.1 LA INFORMACIÓN

La ORGANIZACIÓN PARA LA COOPERACIÓN ECONÓMICA Y EL DESARROLLO (OECD) define los principios de la información que deben estar presentes en todos los sistemas y redes de información para que "sean consistentes con los valores de una sociedad democrática, particularmente con la necesidad de contar con flujos de información libres y abiertos, teniendo en cuenta los principios básicos de protección de la privacidad personal"[2].

Los principios de información definidos son:

> **Concienciación**: Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.
> **Responsabilidad**: Todos los participantes son responsables de la seguridad de los sistemas y redes de información.
> **Respuesta**: Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.
> **Ética:** Los participantes deben respetar los intereses legítimos de terceros.
> **Democracia:** La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.
> **Evaluación del riesgo:** Los participantes deben llevar a cabo evaluaciones de riesgo.
> **Diseño y realización de la seguridad:** Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.
> **Gestión de la Seguridad**: Los participantes deben adoptar una visión integral de la administración de la seguridad.
> **Reevaluación:** Los participantes deben revisar y reevaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.[3]

En la operación de una organización se maneja y comparte información y dependiendo de la actividad realizada y del tipo de información procesada, se deberá tratar de forma diferente según su sensibilidad, criticidad y oportunidad.

La información en si es un conjunto de datos específicos que puede presentarse en cualquier medio y puede tener un significado diferente dependiendo del contexto utilizado, lo que permite tomar ciertas decisiones en lugar de otras, con el fin de adquirir un beneficio o reducir la incertidumbre de algo.

---

[2] ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO, Directrices de la OECD para la seguridad de sistemas y redes de información. Paris : OECD, 2002. p.7.
[3] Ibid., p. 8.

La información puede representarse de varias formas, ya sea en un documento físico o en un archivo electrónico. En general son datos que fluyen por los procesos organizacionales siendo administrada y procesada por personas o sistemas de información.

3.1.1 Tipos de información

La información puede diferenciarse por su contenido considerándose los siguientes tipos:

- **Personal:** la información personal Identificable es cualquier información acerca de un individuo mantenida por una organización, incluyendo: cualquier información que pueda ser usada para distinguir o que permita hacer trazabilidad a la identidad de un individuo, tales como el nombre, el número de seguro social, lugar y fecha de nacimiento, número de tarjeta de crédito, de pasaporte, de licencia de conducción o registros médicos, entre otros[4].

- **Comercial:** la información comercial, es la referente a las entidades, empresas, establecimientos, personas jurídicas y en general a los comercios tales como el Nombre o razón social, dirección, teléfono, fax, representante legal, actividad económica, información financiera, etc.

Adicionalmente, la información puede tener asociado un grado de sensibilidad según el tipo y la cantidad de datos que contengan, por lo que se han diferenciado tres tipos con el fin de proteger las personas, instituciones, entidades o cualquier individuo al que se haga referencia con dicha información[5]:

- **Pública**: la información puede ser considerada pública cuando los datos contenidos en ella sean de esta naturaleza, teniendo en cuenta que su puede estar establecida como pública por mandatos de la ley o de la constitución política, puede ser comunicada sin restricciones ni autorizaciones previas sin causar daño al titular o terceras personas si se llegase a hacer pública y su intención es que sea de uso público.

- **Semiprivada:** La información puede ser considerada como semiprivada cuando los datos contenidos en ella no tengan naturaleza íntima, reservada ni pública, y pueda interesar además del titular a un cierto grupo de

[4]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to protecting the confidentiality of personally identifiable information. NIST SP 800-122. Gaithersburg, Estados Unidos : NIST, 2010. p. 2-2.

[5] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 (31, diciembre, 2008). por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la Información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios y la proveniente de terceros países y se dictan otras disposiciones. Bogotá: El Congreso, 2008. p.2

personas o sectores, teniendo en cuenta que puede llegar a requerir autorización expresa del titular de la información para ser consultada, debe existir un propósito específico por parte de los terceros que requieran consultar dicha información y podría causar efectos negativos al titular o a terceras personas si su contenido llegase a ser publicado sin autorización.

- **Privada:** La información es considerada privada cuando los datos contenidos en ella sean de esta naturaleza y sólo concierne al titular de la información, teniendo en cuenta es información que requiere de autorización expresa del titular de la información para ser consultada y causaría efectos negativos al titular o a terceras personas si su contenido llegase a ser publicado sin autorización.

Algunos ejemplos de activos que pueden contener estos tipos de información dentro de una organización son:

Tabla 1. Ejemplo de activos por tipo de información

Tipo de información	Activos
Información pública	Documentos públicos Sentencias judiciales que no estén sometidas a reserva Estado civil de las personas Estatutos y estados financieros Políticas y condiciones de uso de un servicio Portales web Resoluciones y Leyes del estado
Información semiprivada	Documentos de procedimientos organizacionales Bases de datos de clientes Listas de precios Políticas organizacionales
Información privada	Libros de contabilidad Planes estratégicos Actas de junta directiva Registros de nómina

Fuente Elaboración propia

3.1.2 Propiedades de la Información

La relevancia de la información difiere debido a su contenido y propósito, por lo que es indispensable que se controle y mantenga el acceso a los datos de forma

restringida y autorizada manteniendo los datos íntegros y disponibles según dicha relevancia.

Las propiedades mínimas de la información que se definen dentro de este modelo son la confidencialidad, integridad y disponibilidad, ya que en estas se puede integrar en su mayoría todas las directrices de la información definidas por la OECD.

Tabla 2. Propiedades de la información

Propiedades	Definición FISMA	Definición ISO 27001	Definición FIPS 199
Confidencialidad	Preservar las restricciones autorizadas sobre el acceso de la información y su divulgación, teniendo en cuenta la protección de la información privada y de la propiedad de la información	Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados	Una pérdida de confidencialidad es la divulgación no autorizada de la información. .
Integridad	Proteger contra la modificación inapropiada de la información o su destrucción e incluye asegurar el no repudio y la autenticidad de la información"	Propiedad de salvaguardar la exactitud y estado completo de los activos.	Una pérdida de integridad es una modificación no autorizada o destrucción de la información.
Disponibilidad	Asegurar el acceso confiable a la información y su uso de forma oportuna	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.	La pérdida de disponibilidad es la interrupción del acceso o del uso de la información o de un sistema de información.

Fuente FIPS Publication 199. Standards for Security Categorization of Federal Information and Information Systems

3.2 LA INFORMACIÓN Y LOS ACTIVOS

La información que se maneja en una organización está soportada en diferentes elementos que permiten el flujo de los datos y el acceso a esta por parte de los empleados, clientes y terceros que deberán ser gestionados y mantenidos adecuadamente para dar cumplimiento a los principios de seguridad de la información que contienen o soportan.

En la seguridad de la información, estos elementos son catalogados como Activos ya que representan un valor para la organización, y debido a que se pueden encontrar elementos que se diferencian entre ellos dependiendo de su naturaleza, uso y funcionalidad se han tipificado en los siguientes tipos:

- Activos tipo información

- Activos tipo Software
- Activos tipo Físico
- Activos tipo instalaciones físicas
- Activos tipo personas
- Activos tipo servicios

El valor de los activos estará dado debido a su incidencia en la ejecución de las actividades y las implicaciones que podrían llegar a tener la organización si no se conserva en el estado deseado.

3.2.1 Clasificación de los activos

La Norma ISO/IEC 27001:2005 de la INTERNATIONAL STANDARD ORGANIZATION[6] ha establecido como objeto de control la implementación de un proceso de clasificación de los activos en cuanto a su valor, requisitos legales, sensibilidad y criticidad para la organización. Para realizar una adecuada clasificación es necesario tener claridad en lo que significan estos conceptos en el ámbito de la seguridad de la información:

- **El valor** del activo se determina por la importancia que tiene la información contenida en este. Se puede medir en términos del esfuerzo que conlleva la obtención de dicha información o en el costo económico.
- **Los requisitos legales** deben de reconocerse debido a la naturaleza de la información que puede ser manejada dentro del negocio, tal como la información personal, pública, financiera, información protegida por derechos de autor o de propiedad intelectual.
- **La sensibilidad** del activo debe ser determinada en cuanto al impacto que tendría que personas no autorizadas tuvieran acceso al mismo.
- **La criticidad** como criterio de clasificación de los activos, debe evaluarse en cuanto a que tan indispensable es el activo para mantener el flujo de la información y su disponibilidad.

Por medio de la clasificación se puede establecer donde está concentrada la información y cual debe de protegerse debido a su valor, sensibilidad y criticidad para el negocio, permitiendo así que ejercicios de análisis de riesgos, de prevención de fuga de información, de establecimiento de roles de operación crítica, y otras iniciativas posibles, ya que se conoce cuales son los activos que soporta la organización, donde están y su importancia.

[6] INTERNATIONAL STANDARD ORGANIZATION. Op. cit., p. 15.

3.3 MODELOS DE CLASIFICACIÓN DE REFERENCIA

Alrededor del mundo existen diferentes instituciones y organizaciones que trabajan continuamente en el desarrollo y estandarización de conceptos y métodos que permiten gestionar la seguridad de la información en las organizaciones.

Algunas de ellas, han trabajado específicamente en la definición de metodologías orientadas al análisis de riesgos de seguridad de la información, planteando esquemas específicos de cómo realizar el inventario y la evaluación de los activos con el fin de clasificarlos según el valor que este represente al negocio y al propósito específico de mantener la seguridad de la información.

Se encontraron tres modelos que se aproximan a las necesidades planteadas en este trabajo y para su determinación, se hizo el análisis del alcance en cuanto a la descripción y los tipos de activos que permite identificar, las dimensiones de seguridad consideradas y los aspectos organizacionales sobre los cuales se mide el impacto causado por las degradaciones que puedan presentar los activos identificados.

Al final de este trabajo se planta una discusión de las ventajas y desventajas de cada modelo respecto al planteamiento del problema y otros aspectos de análisis de interés para el marco de la Seguridad de la información.

3.3.1 MEHARI 2010

MEHARI es un método para la evaluación y gestión de riesgos elaborada por el CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS (CLUSIF)[7] que plantea el análisis por medio de la identificación de situaciones de riesgo que pueden presentarse en cada uno de los procesos de la organización que tengan una probabilidad realista de ocurrir.

Los escenarios de riesgo son situaciones que se presentan por fallas funcionales de la integridad, confidencialidad o disponibilidad del proceso y de su información que puedan generar situaciones críticas para la organización. El impacto de estas fallas funcionales se debe describir luego en cuatro (4) niveles de impacto, relacionando las implicaciones que pudiera tener para la operación, imagen y economía de la organización su ocurrencia.

Estas fallas funcionales pueden ser ocasionadas por fallas técnicas que se presenten sobre los recursos y soportes que se utilizan para el manejo de la información por lo que también deben relacionarse las posibles fallas técnicas de los activos utilizados en los procesos.

[7] CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS. Méthode harmonisée d'analyse des risques. MEHARI 2010. París : CLUSIF, 2010.

Los activos identificados se dividen en tres tipos que son los Servicios, los Datos y los de Gestión del proceso, por cada uno de los activos identificados dentro de estos tipos, se evalúa el impacto que generarían a la organización la pérdida de su confidencialidad, integridad o disponibilidad considerando su implicación en las situaciones de riesgo identificadas inicialmente.

Al final se tienen tres tablas de clasificación de activos, una por cada tipo, y su valoración de impacto por cada proceso de negocio. El valor total de la clasificación por activo, será el de mayor impacto de todas las evaluaciones.

3.3.2 MARGERIT V2

MARGERIT es la metodología de riesgos elaborada por el CONSEJO SUPERIOR DE ADMINISTRACION ELECTRÓNICA (CSAE)[8] para la medición de riesgos de seguridad de las entidades y organizaciones españolas, el cual está en conformidad con la Norma ISO/IEC 27001:2005.

El primer paso que describe para el análisis de riesgos es la identificación de activos que divide en ocho tipos y sobre los cuales plantea la dependencia que existe entre estos, para que sean tenidas en cuenta al momento de hacer la valoración del impacto.

Las dimensiones de seguridad que plantea son la confidencialidad, integridad, disponibilidad, autenticidad, la trazabilidad al acceso de los datos y la trazabilidad al uso de los servicios y establece una escala de valor de los impactos generados en la seguridad de las personas, en el cumplimiento, la economía, la operación, la capacidad de la identificación de delitos y otros, planteando así una escala de 10 niveles de valoración de impacto.

La clasificación se hace sólo sobre aquellos activos que están en el nivel superior de dependencias y luego por valor acumulado, los activos dependientes, asumirán el valor de impacto de los activos superiores a él. La evaluación del impacto se realiza en todas las dimensiones de seguridad para los activos tipo datos y servicios, mientras que para el resto de los activos, sólo se valora la disponibilidad.

3.3.3 NIST SP 800-60

El NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)[9] definió la guía de mapeo de información y de sistemas de información en categorías de

[8] CONSEJO SUPERIOR DE ADMINISTRACION ELECTRÓNICA. . Metodología de análisis y gestión de riesgos de los sistemas de información. MARGERIT V2. Madrid : CSAE, 2006.

[9] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide for mapping types of information and informations Systems to security categories. NIST SP 800-60. Gaithersburg, Estados Unidos : NIST, 2008

seguridad, dependiendo del tipo de información y su implicación en procesos misionales de las agencias federales.

Reconoce como objetivos de seguridad la protección de la confidencialidad, integridad y disponibilidad de la información identificando tres niveles de impacto sobre aspectos como la operación los individuos y los activos organizacionales.

El objeto de clasificación es la información en sí misma, tipificándola en cuatro tipos según su propósito y contenido que son: Misional, Entrega del servicio, Procesos de gestión y Mandatos legislativos.

La clasificación de cada tipo de información identificada se hace evaluando uno a uno los impactos generados a la organización situaciones que afecten la confidencialidad, integridad y disponibilidad de la información.

4 MODELO DE CLASIFICACIÓN

El modelo de clasificación se establece conforme a la Norma ISO/IEC 27001:2005 que especifica los requisitos mínimos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información a partir de la definición e implementación de controles.

El dominio Gestión de Activos tiene por objetivo definir la responsabilidad de los activos y clasificarlos según su importancia para lo que propone varios controles que deben de considerarse implementar.

Figura 1. Controles del Dominio de Gestión de activos

A.7 GESTIÓN DE ACTIVOS		
A.7.1 Responsabilidad por los activos Objetivo: lograr y mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	Inventario de activos	Control Todos los activos se deben identificar claramente y se debe elaborar y mantener un inventario de todos los activos importantes.
A.7.1.2	Dueños de los activos	Control Toda la información y activos asociados con las instalaciones de procesamiento de información deben tener un "dueño[3]", que es la parte designada de la organización.
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de información y activos asociados con las instalaciones de procesamiento de información
A.7.2 Clasificación de la información Objetivo: asegurar que la información reciba un nivel apropiado de protección.		
A.7.2.1	Directrices para clasificación	Control La información se debe clasificar en cuanto a su valor, requisitos legales, sensibilidad y criticidad para el sistema.
A.7.2.2	Etiquetado y manejo de información	Control Se debe desarrollar e implementar un conjunto apropiado de procedimientos para etiquetado y manejo de la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Fuente NTC ISO 27001

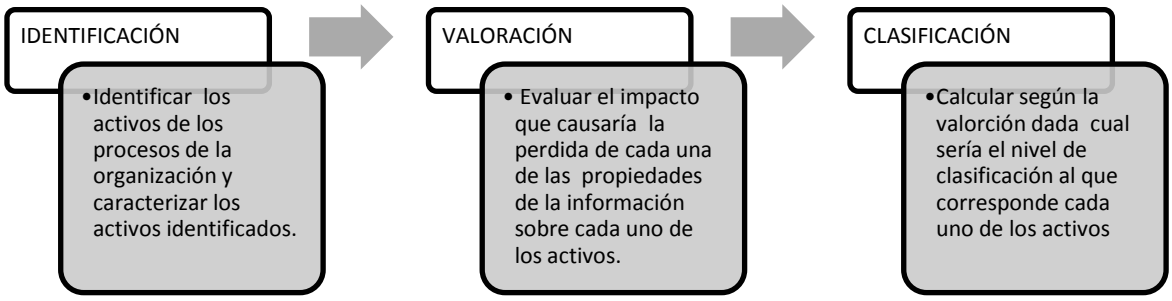
Por este motivo, la clasificación debe de tener ciertos requerimientos para alinearse a los controles definidos por la norma, siendo estos la definición de los dueños de la información, las directrices de clasificación, el uso aceptable, el etiquetado y manejo de la información.

El modelo de clasificación establece como deben identificarse los activos que soportan la información dentro de una organización de forma estructurada y

sistemática para valorar el nivel de confidencialidad, integridad y disponibilidad determinando los directrices de clasificación acorde con los aspectos organizacionales más relevantes.

La ventaja de este modelo es que la organización podrá determinar desde un inicio el nivel de importancia que tiene la integridad, confidencialidad y disponibilidad de la información así como así como los diferentes aspectos organizacionales que pueden verse afectados, basándose en su actividad económica para obtener una clasificación de los activos acorde con la protección de la información que se mantiene al interior de la organización.

Figura 2. Fases del modelo de clasificación



FUENTE Elaboración propia

4.1 IDENTIFICACIÓN DE LOS ACTIVOS

Los activos son todos los recursos que se emplean para realizar el procesamiento, almacenamiento y en general todo el mantenimiento de la información, desde su creación hasta su destrucción.

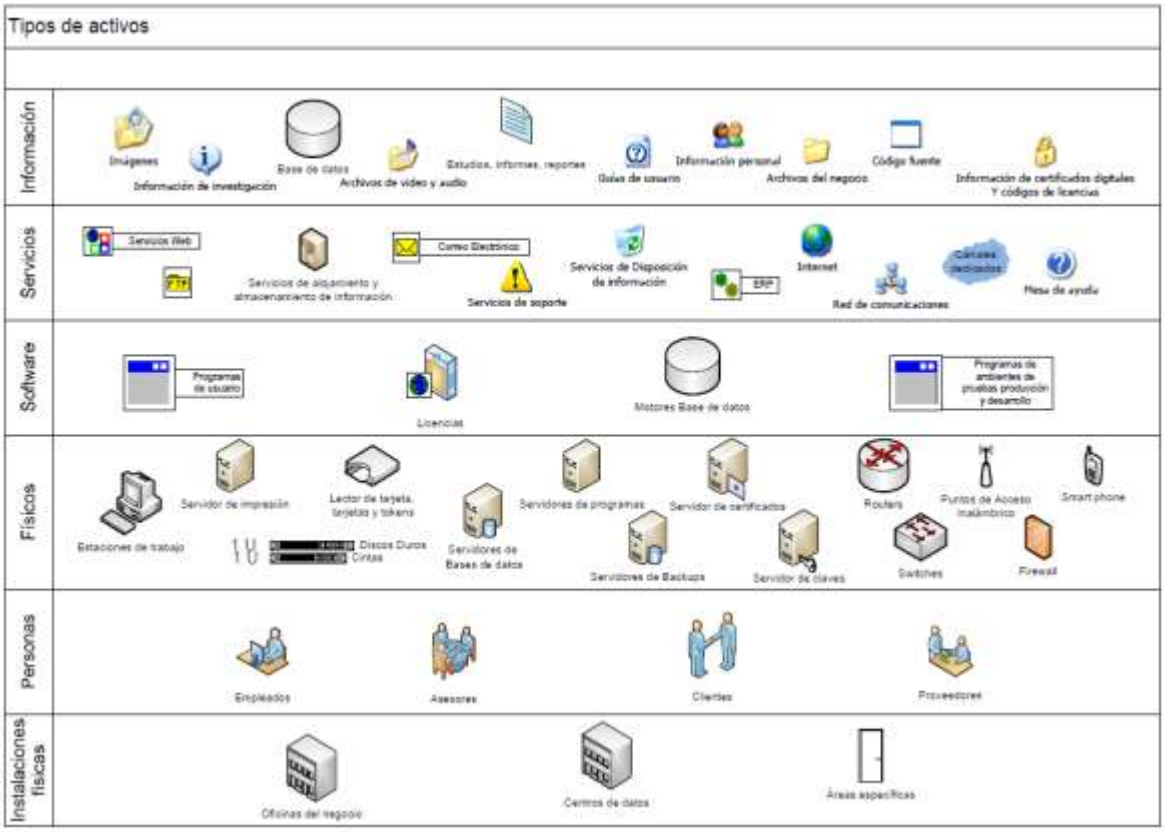
La identificación de los activos, se realizará empezando por identificar toda la información que se maneja al interior de la organización, tanto de forma digital como física, analizando cuales son las actividades realizadas y los elementos tecnológicos y físicos utilizados en dicha interacción.

Basándose en un modelo de capas la información se ubica en la cima ya que es el objeto principal de protección y luego, uno a uno los tipos de información se van identificando teniendo en cuenta el soporte que brindan para acceder y manejar la información.

Por medio de este modelo se identifica la relación que existen entre los diferentes tipos de activos lo cual debe tenerse en cuenta en la evaluación del impacto sobre la organización ya que se podrá determinar cuál es la información afectada del negocio.

Todos estos elementos considerados activos permiten el flujo de la información de la organización y deben clasificarse teniendo en cuenta su propósito y su implicación dentro del procesamiento de la información. La siguiente figura representa los diferentes tipos de activos que se pueden encontrar en sus respectivas capas.

Figura 3. Tipos de activos



Fuente Elaboración propia

4.1.1 Activos tipo Información

La **información** son todos los datos que se requieren para la ejecución de los procesos de la organización, los cuales pueden estar en formato digital o físico como las bases de datos y archivos de datos, contratos y acuerdos, documentos, manuales de usuario, procedimientos operativos o de soporte, planes de continuidad del negocio, acuerdos de recuperación, registros de auditoría, actas, claves, contraseñas, llaves públicas y privadas y códigos fuentes de desarrollos.

4.1.2 Activos tipo servicios

Son los **servicios** con los que se cuenta para el desarrollo de las actividades y el manejo de la información por parte de personal interno o externo a la Organización siendo estos los servicios de computación y comunicaciones, servicios de soporte, servicios de impresión, servicios de correspondencia, servicios de almacenamiento, servicios de información especializada del negocio y servicios generales.

4.1.3 Activos tipo software

Es el conjunto de **aplicativos, programas** y **ejecutables** que son requeridos para la implementación de los servicios que permiten la interacción con la información del negocio de forma ordenada y sistemática, facilitando su uso como software de aplicación, sistemas operativos, herramientas de desarrollo, utilidades del sistema, licencias de productos y motores de bases de datos.

4.1.4 Activos tipo físicos

Estos activos son los elementos que soportan los sistemas de información, las redes de comunicaciones y los sistemas de almacenamiento y en general todos los servicios identificados.

- **Los medios de almacenamiento y procesamiento de información** son los dispositivos que almacenan, procesan y albergan los aplicativos y la información soportando así la prestación de los servicios y el funcionamiento de los sistemas de información que usan las personas del proceso en la ejecución de sus actividades

- **Equipos de comunicaciones** se refiere a todos los elementos informáticos que permiten el flujo de los datos y el intercambio de la información. Estos equipos son los que interconectan a los equipos de almacenamiento y procesamiento de la información, con las estaciones de usuario y terceros que hagan parte del proceso.

4.1.5 Activos tipo instalaciones físicas

Son las **locaciones** donde se ubican los equipos de almacenamiento, procesamiento y comunicaciones, así como la información física de la organización que debe contar con las condiciones necesarias para el correcto funcionamiento de los servicios y sistemas de información identificados.

Ejemplos de este tipo de activos son: centros de datos, centros alternos, oficinas, edificios y bodegas.

4.1.6 Activos tipo personas

Son los **individuos** que administran, manejan, procesan y utilizan los activos de la organización considerando a los internos y externos como proveedores, contratistas, prestadores de servicios y clientes, siendo en general todos los que tienen acceso a la información o la mantienen disponible.

Los activos tipo personas son los empleados de la organización, proveedores, clientes, contratistas, consultores y otras empresas u organizaciones.

4.1.7 Activos tipo intangibles

Son activos de **naturaleza inmaterial** susceptibles a ser gestionados y que aportan valor, derecho o privilegio a la organización. El conocimiento de los empleados, aportan un valor agregado a los servicios o productos que ofrezca la organización, puesto que es el diferenciador haciéndolo diferenciarse de la competencia, y deberá considerarse como activo en cuanto que aporta valor al negocio.

La imagen o reputación que la empresa construya a través del tiempo que permanezca en el mercado es un activo ya que proporciona confiabilidad en sus clientes y posicionamiento entre empresas del mismo sector, apuntando al liderazgo de la organización entre las organizaciones que puedan ofrecer los mismos productos o servicios.

También los procesos son considerados como activos intangibles puesto que representan el conjunto de actividades que se sigue en un determinado momento para dar soporte al objeto de negocio.

Otros activos intangibles que deben considerarse puesto a que representan información de la organización son los derechos de autor, de propiedad intelectual, marcas, cultura corporativa, secretos comerciales, competencias, reputación, imagen y patentes.

4.2 VALORACIÓN DE LAS PROPIEDADES DE LA INFORMACIÓN

Las propiedades fundamentales de la información deben ser mantenidas en los niveles adecuados para evitar que se presenten situaciones que afecten al negocio negativamente, por lo tanto su interpretación debe diferenciarse según el tipo de activo que se está valorando y las implicaciones que podrían llegar a tener la pérdida de sus propiedades.

4.2.1 Afectación a la disponibilidad

La disponibilidad sobre los activos debe ser evaluada respecto al nivel de impacto que pueda presentarse por una interrupción al acceso de la información que dicho activo contenga o soporte ya que podría causar retrasos en la ejecución de procesos e incapacidad de hacer verificación de la información, exponiéndose a repercusiones legales o internas para la organización.

La pérdida de disponibilidad se presenta de forma diferente sobre cada tipo de activo:

- **Información:** la no disponibilidad está reflejada en la falta de acceso a la información de la organización que es utilizada en sus procesos.
- **Servicios**: la no disponibilidad de los servicios es la falta de prestación de dicho servicio, la cual puede ser ocasionada por la falla de los elementos que la componen.
- **Software**: la no disponibilidad del software está reflejada al no tener acceso a las aplicaciones que son usadas en los sistemas de información de la organización o a los sistemas operativos de equipos tecnológicos.
- **Físicos**: la no disponibilidad del hardware es el daño del activo o de cualquiera de sus componentes de forma que no permita su funcionamiento o ponga en riesgo el acceso oportuno a la información.
- **Personas**: la no disponibilidad es de las personas es que no se encuentre en el momento que sea requerida su intervención dentro de la ejecución del proceso y no se pueda completar la actividad desde el punto de vista organizacional, identificando el rol que desempeña dentro del proceso.
- **Intangibles:** la no disponibilidad es considerada como la pérdida del activo intangible.

4.2.2 Afectación a la Integridad

La integridad como propiedad de la información, se refiere a la confiabilidad que deben tener los activos para garantizar que el flujo de la información y la ejecución de los procesos se completen satisfactoriamente.

Los cambios no autorizados que se realicen sobre los activos podrían generar graves consecuencias directas como la modificación de una entrada financiera, de una alerta médica, o de antecedentes penales o indirectas como la facilitación del acceso no autorizado a un servicio de información privada o al sistema operativo de un servidor de aplicación o el empleo de un sistema como sustituto de los ataques hacia otros sistemas.

Según el tipo de activo, la pérdida de integridad se identifica como:

- **Información:** la pérdida de integridad de la información se refiere a la alteración de los datos de forma no controlada o la eliminación parcial de registros o campos específicos de documentos, bases de datos, códigos ejecutables, programas fuente.
- **Software**: la pérdida de integridad del software se refiere a cuando se presenta un funcionamiento inadecuado de las aplicaciones como la ausencia de información específica dentro de la interfaz de la aplicación que permite acceder a la información.
- **Físicos**: la pérdida de integridad de los activos físicos se refiere al mal funcionamiento de forma parcial de alguno de sus componentes que no afectan la disponibilidad del activo pero si afectan el normal flujo de los procesos o de la información para los que están dispuestos.
- **Servicios**: la pérdida de integridad de los servicios se refiere al incorrecto funcionamiento o prestación del servicio de forma inadecuada.
- **Personas**: la pérdida de integridad de las personas se refiere a cuando por motivos intencionales o no proporcionen información incorrecta o incompleta en su participación dentro del proceso.
- **Intangibles:** la pérdida de integridad de los intangibles se refiere a cuando estos activos se degradan de forma que puedan interpretarse adecuadamente y transmitir mensajes errados.

4.2.3 Afectaciones a la confidencialidad

Debido a que los activos pueden contener información que sea sensible para el negocio o para un grupo de personas específico, debe de valorarse cuál sería el impacto causado si esta llega a ser conocida por personas ajenas al proceso que no estén autorizadas ya sea accidental o intencionalmente.

La divulgación no autorizada de la información puede conllevar a la modificación no autorizada, destrucción de la información o a la negación de los servicios, llegando al incumplimiento de leyes, órdenes ejecutivas o regulaciones que debe cumplir la organización.

Según el tipo de activo, la pérdida de confidencialidad debe verse como:

- **Información**: la pérdida de confidencialidad se trata como el conocimiento no autorizado o la divulgación intencional o no intencional de la información de forma inoportuna que se encuentre contenida en los documentos, bases de datos, códigos fuentes, archivos de datos, estrategias, políticas, tarifas, comunicados o de cualquier activo de este tipo.

- **Software:** la pérdida de confidencialidad del software se interpreta como el acceso a las aplicaciones de la organización o a programas de forma no autorizada.
- **Físicos**: la pérdida de confidencialidad de los activos físicos se interpreta como el acceso de personas no autorizadas al activo y a partir de esta este obtenga acceso a la información.
- **Servicios:** la pérdida de confidencialidad de los servicios se interpreta como el acceso no autorizado al servicio o sistema de información
- **Personas:** la pérdida de confidencialidad de las personas es cuando de forma intencional o no, divulguen información de sus funciones laborales o de la información que manejan en sus actividades.
- **Intangibles:** la pérdida de confidencialidad de los activos intangibles, se presenta cuando de forma intencional o no se divulga su contenido.

4.2.4 Impacto a la organización

Cada vez que se presenta una situación que afecta la confidencialidad, integridad o disponibilidad de la información se pone en riesgo a la organización, ya que se podrían ver afectados diferentes aspectos que componen la estructura de una organización.

El modelo contempla el impacto sobre la operación, la economía y el cumplimiento de una organización ya que estos se han identificado como pilares fundamentales en el mantenimiento y establecimiento de objetivos de negocio de la mayoría de las organizaciones, sobre los cuales se identificará el grado de impacto que pueden sufrir dependiendo del tipo de activo y propiedad degradada.

Tabla 3. Aspectos organizacionales

OPERACIÓN	ECONOMÍA	CUMPLIMIENTO
En el aspecto operativo se tiene en cuenta todos los procesos y activos que mantienen la continuidad del negocio. En este caso se hace referencia a las tareas o actividades que se realizan, las personas, los activos físicos que soportan la operación y los servicios que se utilizan o que se brindan.	El aspecto económico describe el mantenimiento de las finanzas en los niveles deseados y esperados por la organización. Hace referencia a la capacidad de pago de responsabilidades y el detrimento que pueden sufrir estas por consecuencia de resultados inesperados.	Se refiere al cumplimiento que la organización debe estar alineada como leyes, regulaciones y normas definidas por entes externos, así como el cumplimento de políticas, acuerdos y contratos.

Fuente Elaboración propia

Todos y cada uno de los activos identificados deben ser evaluados por cada una de las propiedades identificando el impacto que puede generar la pérdida de confidencialidad, integridad o disponibilidad del activo a la operación, la economía y el cumplimiento individualmente, ya que es posible que el nivel de impacto causado a la operación sea diferente al causado a la economía o al cumplimiento.

Por cada una de las propiedades de la información debe seleccionar el nivel de impacto que puede causar en la operación, economía o cumplimiento de la organización y sólo podrá ser elegido un nivel de impacto por cada propiedad.

Tabla 4. Impacto operativo

	OPERATIVO				
	MÍNIMO (1)	**BAJO (2)**	**MEDIO (3)**	**ALTO (4)**	**MUY ALTO (5)**
Confidencialidad	La pérdida de confidencialidad del activo afecta casi de forma imperceptible la operación de los procesos de la organización, las personas y el flujo de la información.	La pérdida de confidencialidad del activo afecta de cierta forma la operación de los procesos de la organización, las personas y el flujo de la información.	La pérdida de confidencialidad del activo afecta la operación de los procesos de la organización, las personas y el flujo de la información.	La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información.	La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información.
Integridad	La pérdida de integridad del activo afecta casi de forma imperceptible la operación de los procesos de la organización, las personas y el flujo de la información.	La pérdida de integridad del activo afecta de cierta forma la operación de los procesos de la organización, las personas y el flujo de la información.	La pérdida de integridad del activo afecta la operación de los procesos de la organización, las personas y el flujo de la información.	La pérdida de integridad del activo afecta considerablemente afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información.	La pérdida de integridad del activo afecta totalmente afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información.
Disponibilidad	La pérdida de disponibilidad del activo afecta casi de forma imperceptible la operación de los procesos, de la organización, las personas y el flujo de la información.	La pérdida de disponibilidad del activo afecta de cierta forma la operación de los procesos, de la organización, las personas y el flujo de la información.	La pérdida de disponibilidad del activo afecta la operación de los procesos, de la organización, las personas y el flujo de la información.	La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos, de la organización, las personas y el flujo de la información.	La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos, de la organización, las personas y el flujo de la información.

Fuente Elaboración propia

Tabla 5. Impacto económico

	ECONÓMICO				
	MÍNIMO (1)	**BAJO (2)**	**MEDIO (3)**	**ALTO (4)**	**MUY ALTO (5)**
Confidencialidad	La pérdida de confidencialidad del activo afecta casi de forma imperceptible las finanzas de la organización.	La pérdida de confidencialidad del activo afecta de cierta forma las finanzas de la organización.	La pérdida de confidencialidad del activo afecta las finanzas de la organización.	La pérdida de confidencialidad del activo afecta considerablemente las finanzas de la organización.	La pérdida de confidencialidad del activo afecta totalmente las finanzas de la organización.
Integridad	La pérdida de integridad del activo afecta casi de forma imperceptible las finanzas de la organización.	La pérdida de integridad del activo afecta de cierta forma las finanzas de la organización.	La pérdida de integridad del activo afecta las finanzas de la organización.	La pérdida de integridad del activo afecta considerablemente las finanzas de la organización.	La pérdida de integridad del activo afecta totalmente las finanzas de la organización.
Disponibilidad	La pérdida de disponibilidad del activo afecta casi de forma imperceptible las finanzas de la organización.	La pérdida de disponibilidad del activo afecta de cierta forma las finanzas de la organización.	La pérdida de disponibilidad del activo afecta las finanzas de la organización.	La pérdida de disponibilidad del activo afecta considerablemente las finanzas de la organización.	La pérdida de disponibilidad del activo afecta totalmente las finanzas de la organización.

Fuente Elaboración propia

Tabla 6. Impacto cumplimiento

	CUMPLIMIENTO				
	MÍNIMO (1)	**BAJO (2)**	**MEDIO (3)**	**ALTO (4)**	**MUY ALTO (5)**
Confidencialidad	La pérdida de confidencialidad del activo afecta casi de forma imperceptible la reputación, imagen o las finanzas de la organización.	La pérdida de confidencialidad del activo afecta de cierta forma la reputación, imagen o las finanzas de la organización.	La pérdida de confidencialidad del activo afecta la reputación, imagen o las finanzas de la organización.	La pérdida de confidencialidad del activo afecta considerablemente la reputación, imagen o las finanzas de la organización.	La pérdida de confidencialidad del activo afecta totalmente la reputación, imagen o las finanzas de la organización.
Integridad	La pérdida de integridad del activo afecta casi de forma imperceptible la reputación, imagen o las finanzas de la organización.	La pérdida de integridad del activo afecta de cierta forma la reputación, imagen o las finanzas de la organización.	La pérdida de integridad del activo afecta la reputación, imagen o las finanzas de la organización.	La pérdida de integridad del activo afecta considerablemente la reputación, imagen o las finanzas de la organización.	La pérdida de integridad del activo afecta totalmente la reputación, imagen o las finanzas de la organización.
Disponibilidad	La pérdida de disponibilidad del activo afecta casi de forma imperceptible la reputación, imagen o las finanzas de la organización.	La pérdida de disponibilidad del activo afecta de cierta forma la reputación, imagen o las finanzas de la organización.	La pérdida de disponibilidad del activo afecta la reputación, imagen o las finanzas de la organización.	La pérdida de disponibilidad del activo afecta considerablemente la reputación, imagen o las finanzas de la organización.	La pérdida de disponibilidad del activo afecta totalmente la reputación, imagen o las finanzas de la organización.

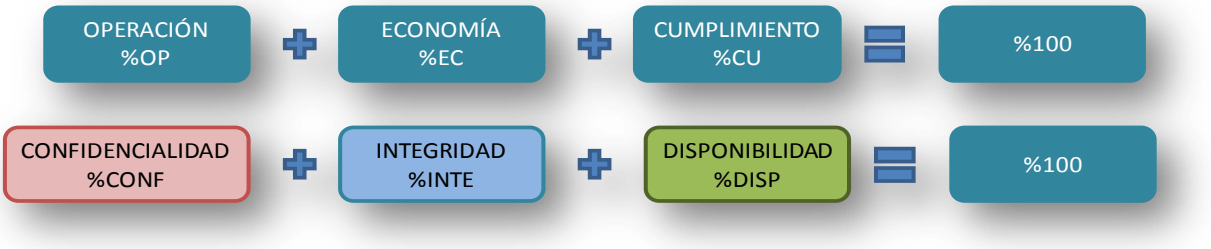
Fuente Elaboración propia

4.3 CLASIFICACIÓN DE LOS ACTIVOS

4.3.1 Ponderación del modelo

Para que la clasificación tenga en cuenta las actividades y objetivos del negocio, se debe de asignar un peso a cada una de las variables del modelo con el fin de darle mayor, menor o la misma relevancia.

Figura 4. Ponderación



Fuente Elaboración propia

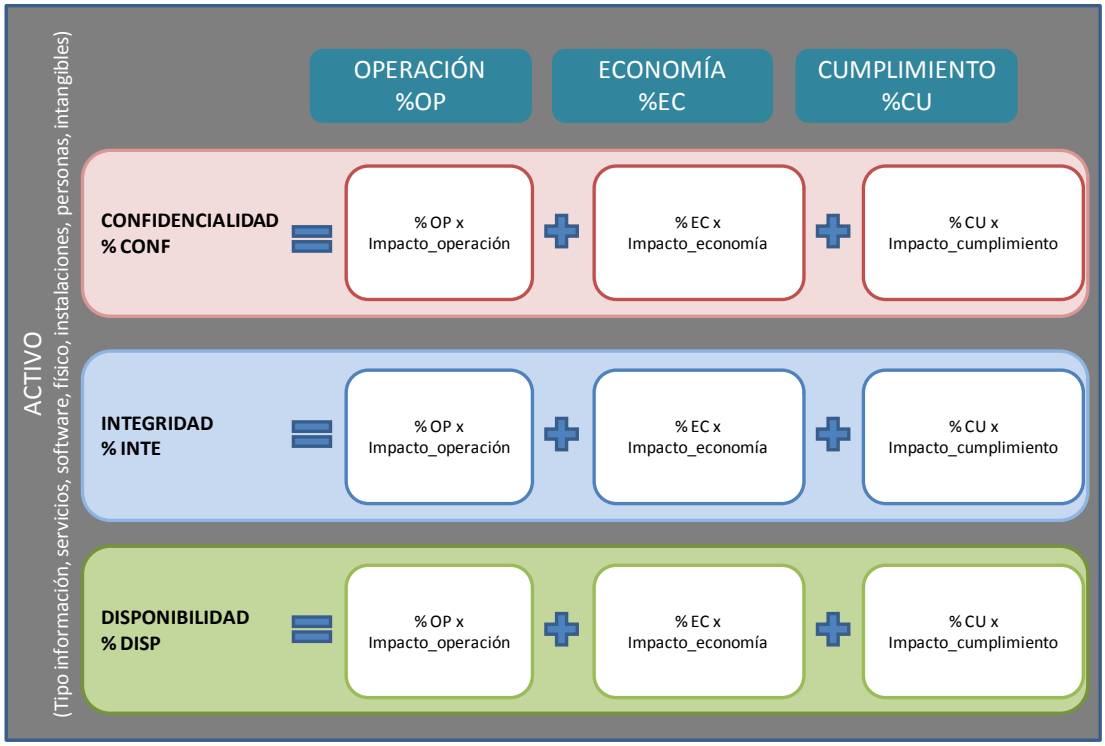
La operación podrá ser más relevante para organizaciones que sean prestadoras de servicios públicos o de producción, mientras que el cumplimiento podrá ser más relevante para el sector gobierno, igualmente, la confidencialidad será más importante en las organizaciones del sector financiero mientras que al integridad sea lo más importante para el sector legal por lo tanto la ponderación permite que la clasificación de los activos tenga en cuenta las afectaciones en estos aspectos y priorice los más relevantes.

4.3.2 Clasificación por propiedad

Cada una de las propiedades de la información ha sido valorada según el impacto causado en la operación, economía y cumplimiento teniendo en cuenta su ponderación, por lo que se tendrán tres valores por cada una de ellas.

El valor total de clasificación por propiedad será la suma de los impactos generados en cada uno de los aspectos organizacionales para que de esta forma sólo se tenga un valor de clasificación por propiedad del activo tal como se muestra en la siguiente figura.

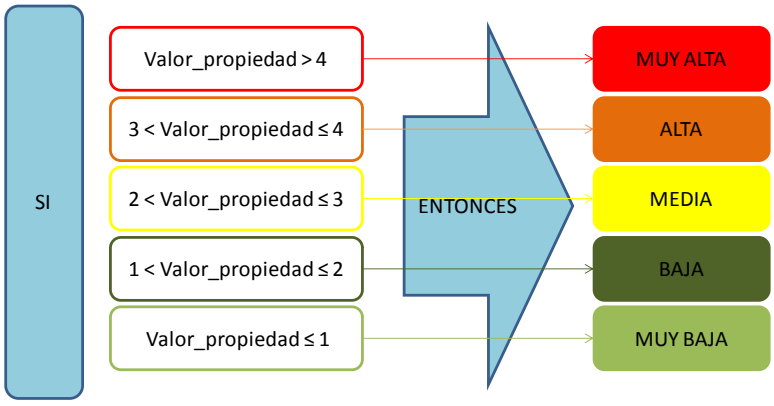
Figura 5. Valor del activo por propiedad



Fuente Elaboración propia

El modelo catalogará el nivel de clasificación a cada propiedad según su resultado en una escala de 5 niveles que determinará la importancia de dicha propiedad sobre el activo de información para la organización.

Figura 6. Conversión a valoración cualitativa



Fuente Elaboración propia

El resultado de esta clasificación por propiedad permite a la organización reconocer el grado de confidencialidad, integridad y disponibilidad que debe tener el activo con el fin que no afecte a la organización

Tabla 7. Definición de los niveles de clasificación por propiedad

	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Confidencialidad	El activo tiene un mínimo grado de sensibilidad para la organización por lo que afecta casi de forma imperceptible la operación, la economía o aspectos de cumplimiento.	El activo tiene un bajo grado de sensibilidad para la organización por lo que afecta de cierta forma la operación, la economía o aspectos de cumplimiento.	El activo tiene un mediano grado de sensibilidad para la organización por lo que afecta la operación, la economía o aspectos de cumplimiento.	El activo tiene un alto grado de sensibilidad para la organización por lo que afecta considerablemente la operación, la economía o aspectos de cumplimiento.	El activo tiene muy alto grado de sensibilidad para la organización por lo que afecta totalmente la operación, la economía o aspectos de cumplimiento.
Integridad	Si el activo no mantiene su integridad afecta casi de forma imperceptible la operación, la economía o aspectos de cumplimiento.	Si el activo no mantiene su integridad afecta de cierta forma la operación, la economía o aspectos de cumplimiento.	El activo debe tener un mediano nivel de integridad porque si no afectaría la operación, la economía o aspectos de cumplimiento.	El activo requiere de un alto nivel de integridad, porque si no afectaría considerablemente la operación, la economía o el aspectos de cumplimiento.	El activo debe tener muy alto nivel de integridad porque si no afectaría totalmente la operación, la economía o aspectos de cumplimiento.
Disponibilidad	El activo no es crítico para la organización y no afecta o afecta casi de forma imperceptible la operación, la economía o el cumplimiento.	El activo tiene criticidad baja para la organización y afecta de cierta forma la operación, la economía o el cumplimiento.	El activo tiene criticidad media para la organización y afecta la operación, la economía o el cumplimiento.	El activo tiene criticidad alta para la organización y afecta considerablemente la operación, la economía o el cumplimiento.	El activo tiene criticidad my alta para la organización y afecta de totalmente la operación, la economía o el cumplimiento.

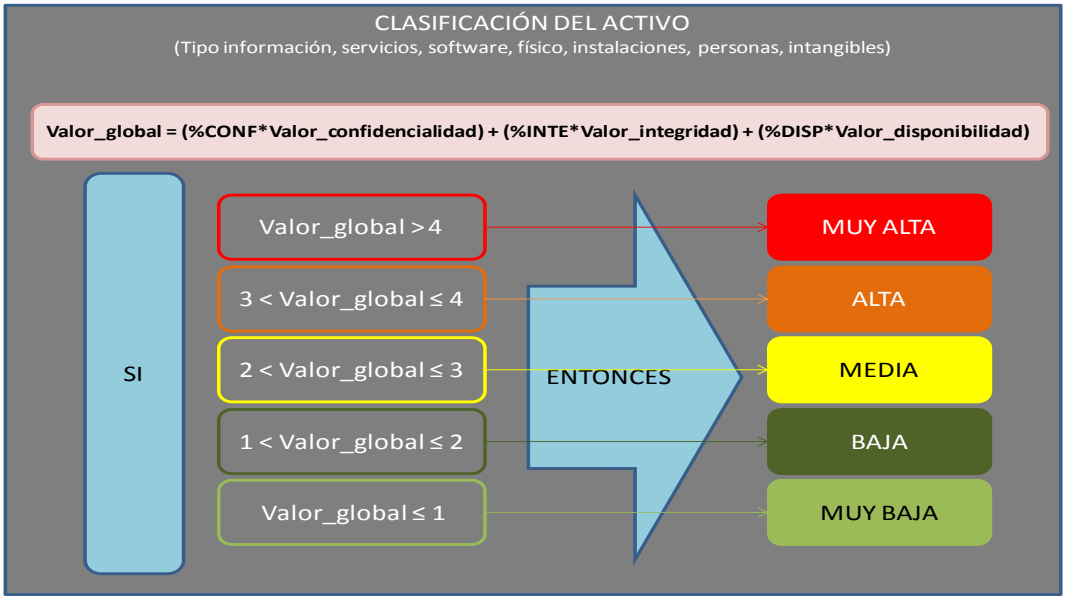
Fuente Elaboración propia

4.3.3 Clasificación total del activo

Una vez se tengan los valores en cada una de las propiedades se hace la clasificación total del activo teniendo en cuenta al igual que en la valoración de los aspectos organizacionales, que previamente se ponderaron las propiedades de la información por lo que debe de multiplicarse los valores de clasificación de la

propiedad por su peso y luego sumarlos para que den como resultado el valor de clasificación del activo total para la organización tal como se muestra en la siguiente figura.

Figura 7. Clasificación total del activo



Fuente Elaboración propia

Con este último paso se obtiene la clasificación total del activo Los posibles niveles de clasificación son definidos en la siguiente escala:

Tabla 8. Definición de los niveles de clasificación total

Clasificación General	Definición de nivel de clasificación
MUY BAJO	No es estrictamente necesario mantener la confidencialidad, integridad y disponibilidad del activo.
BAJO	El mantenimiento de la confidencialidad, integridad y disponibilidad del activo debe realizarse en la medida de lo posible.
MEDIO	Es importante mantener la confidencialidad, integridad o disponibilidad del activo.
ALTO	Mantener la confidencialidad, integridad y disponibilidad del activo es necesario
MUY ALTO	Es indispensable mantener la confidencialidad, integridad y disponibilidad del activo

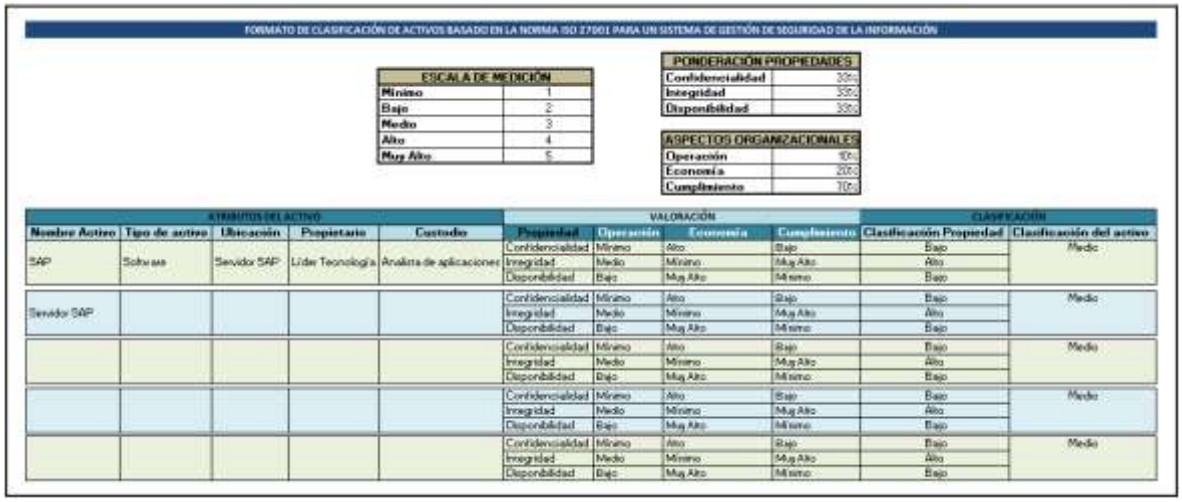
Fuente Elaboración propia

4.3.4 Formato de clasificación

Este formato contiene los campos que son requeridos para garantizar el cumplimiento del objetivo del Dominio A.7 Clasificación de activos de la Norma ISO 27001 y la implementación del modelo de clasificación.

- **Nombre del activo**: Nombre con el cual se reconoce el activo en la organización.
- **Tipo de activo:** Define el tipo al cual pertenece el activo
- **Ubicación del activo:** Puede describir la ubicación tanto física como electrónica del activo.
- **Propietario del activo**: Persona, proceso o grupo de trabajo que tiene la responsabilidad de definir y revisar periódicamente el activo garantizando el mantenimiento de sus propiedades.
- **Custodio del activo:** Persona, proceso o grupo de trabajo encargado de hacer efectivos los controles de seguridad definidos por el propietario.
- **Matriz de valoración:** Zona donde se selecciona el nivel de impacto de la pérdida de las propiedades de los activos sobre los aspectos organizacionales
- **Clasificación:** Resultado de la clasificación por propiedad y total del activo dependiendo de la afectación a las propiedades de la información.

Figura 8. Vista del formato del modelo de clasificación



FORMATO DE CLASIFICACIÓN DE ACTIVOS BASADO EN LA NORMA ISO 27001 PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ESCALA DE MEDICIÓN	
Mínimo	1
Bajo	2
Medio	3
Alto	4
Muy Alto	5

PONDERACIÓN PROPIEDADES	
Confidencialidad	33%
Integridad	33%
Disponibilidad	33%

ASPECTOS ORGANIZACIONALES	
Operación	10%
Economía	20%
Cumplimiento	70%

ATRIBUTOS DEL ACTIVO					VALORACIÓN				CLASIFICACIÓN	
Nombre Activo	**Tipo de activo**	**Ubicación**	**Propietario**	**Custodio**	**Propiedad**	**Operación**	**Economía**	**Cumplimiento**	**Clasificación Propiedad**	**Clasificación del activo**
SAP	Software	Servidor SAP	Líder Tecnología	Analista de aplicaciones	Confidencialidad	Mínimo	Alto	Bajo	Bajo	Medio
					Integridad	Medio	Mínimo	Muy Alto	Alto	
					Disponibilidad	Bajo	Muy Alto	Mínimo	Bajo	
Servidor SAP					Confidencialidad	Mínimo	Alto	Bajo	Bajo	Medio
					Integridad	Medio	Mínimo	Muy Alto	Alto	
					Disponibilidad	Bajo	Muy Alto	Mínimo	Bajo	
					Confidencialidad	Mínimo	Alto	Bajo	Bajo	Medio
					Integridad	Medio	Mínimo	Muy Alto	Alto	
					Disponibilidad	Bajo	Muy Alto	Mínimo	Bajo	
					Confidencialidad	Mínimo	Alto	Bajo	Bajo	Medio
					Integridad	Medio	Mínimo	Muy Alto	Alto	
					Disponibilidad	Bajo	Muy Alto	Mínimo	Bajo	
					Confidencialidad	Mínimo	Alto	Bajo	Bajo	Medio
					Integridad	Medio	Mínimo	Muy Alto	Alto	
					Disponibilidad	Bajo	Muy Alto	Mínimo	Bajo	

Fuente Elaboración propia

5 RESULTADOS

La definición del modelo establece un método de identificación y clasificación de activos conforme a lo establecido en la Norma ISO 27001:2005 que valora los efectos que podría causar a diferentes aspectos de la organización, situaciones que afecten la confidencialidad, integridad y disponibilidad de los activos catalogándolos en diferentes niveles de criticidad que reflejan dicho valor.

Se establece la perspectiva de lo que significa la pérdida de los objetivos de seguridad por cada uno de los tipos de activos referidos para que puedan ser identificadas fácilmente las implicaciones que podrían tener para la organización fallas sistemáticas o individuales de los activos que contienen o soportan la información.

El modelo identifica el impacto causado a cada aspecto de la organización la pérdida de confidencialidad, integridad y disponibilidad de cada activo identificado independientemente y la clasificación total del activo es el resultado de la suma de las valoraciones de impacto en cada uno de los objetivos de seguridad evaluados,

Con el fin que el modelo pueda ser ajustable al objeto de la organización, tanto los criterios de aspectos organizacionales afectados como los objetivos de seguridad, son ponderables para que se asigne el peso correspondiente a la importancias de cada aspecto.

Esta parametrización permite que el modelo pueda ser implementado por empresas de todos los sectores que estén definidas bajo un modelo de procesos y que deseen gestionar la Seguridad de la Información

6 DISCUSIÓN

El desarrollo de los diferentes modelos analizados tienen como factor común que han sido elaborados para dar cumplimiento a lo establecido en la norma ISO 27001, teniendo en cuenta los diferentes tipos de activos que se pueden identificar dentro de un Sistema de Gestión de Seguridad sobre los cuales se analiza el impacto de la pérdida de las dimensiones de seguridad mínimas que se consideran sobre la información que son confidencialidad, integridad y disponibilidad.

Cada uno de estos modelos propone una metodología para la identificación de los activos, su tipificación y el razonamiento para identificar los niveles de impacto causados a la organización, tal como se describió en el Marco teórico. En la siguiente Tabla, se presenta el comparativo entre los modelos que se tomaron como referencia y el modelo que dio como resultado este trabajo investigativo.

Tabla 9. Comparativo de los modelos de clasificación

Modelos	Tipos de activos	Dimensiones de seguridad	Impacto	Aspectos organizacionales evaluados	Clasificación
MARGERIT	[D] datos / información [S] servicios [SW] aplicaciones [HW] equipamiento informático [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar [L] instalaciones [P] personal	[D] disponibilidad [I] integridad [C] confidencialidad [A_S] autenticidad del servicio [A_D] autenticidad de los datos [T_S] trazabilidad del servicio [T_D] trazabilidad de los datos	10 Niveles	Seguridad de las personas Información de carácter personal Cumplimiento Capacidad para la persecución de delitos Intereses comerciales y económicos Pérdidas financieras Interrupción del servicio Orden público Política corporativa	* Activos por Proceso * Dimensión de seguridad por activo
MEHARI 2010	[S] Servicios [D] Datos [MP] Procesos de gestión	[D] disponibilidad [I] integridad [C] confidencialidad	4 niveles	Operación Imagen Economía	* Activos por Proceso * Dimensión de seguridad por activo
NIST 800-60	[M] Misión [ES] Entrega de servicio [MP] Procesos de gestión [CUM] Mandatos legislativos y ejecutivos	[D] disponibilidad [I] integridad [C] confidencialidad	3 Niveles	Operación Activos organizacionales Individuos	* Sistemas de información * Información * Dimensión de seguridad por tipo de información
MODELO PROPUESTO	[D] datos / información [S] servicios [SW] aplicaciones [HW] equipamiento informático [L] instalaciones [P] personal [In] Intangibles	[D] disponibilidad [I] integridad [C] confidencialidad	5 Niveles	Operación Economía Cumplimiento	*Activos por Proceso *Dimensión de seguridad por activo

Fuente Elaboración propia

Analizando el planteamiento del problema que radica en la relevancia que tiene para la clasificación de la información, que el modelo seleccionado plantee claramente la relación que existe entre los activos valorados y las implicaciones

que su pérdida de confidencialidad, integridad y disponibilidad puede tener sobre la organización que los modelos actuales, se identificaron las siguientes ventajas y desventajas de cada modelo respecto al modelo planteado.

MARGERIT es las más completa de las tres analizadas y describe en detalle cada uno de los tipos de activos y las dimensiones de seguridad. Establece la dependencia que existe entre los activos teniendo en cuenta que todos están relacionados con la información y los servicios que se utilizan dentro de una organización, por lo que el valor de un activo que soporte la información objetivo, heredará o tendrá un valor acumulado, dependiendo del valor de dicha información soportada.

Cada una de las dimensiones de seguridad son valoradas dependiendo del activo analizado y establecen que sólo sobre los datos y los servicios deben ser identificados los impactos causados por la pérdida de disponibilidad, integridad, confidencialidad ,trazabilidad y autenticidad, mientras que para el resto de activos, la única propiedad valorada es la disponibilidad.

Esta asociación, se considera un factor de discusión, ya que es posible que activos como ejemplo los tipo Software a pesar de estar disponibles, presenten variaciones en sus parámetros de configuración que afecten la confidencialidad, la integridad o la disponibilidad de la información del negocio que soportan. Esta situación refleja que no sólo hay que analizar la consecuencia si no también la causa, ya que la pérdida de confidencialidad, integridad o disponibilidad de un activo puede afectar de forma diferente e independiente, la confidencialidad, integridad y disponibilidad de la información que soporta.

MEHARI plantea un análisis a partir de la identificación de situaciones de riesgo de pérdida de confidencialidad, integridad o disponibilidad de la información que se puedan presentar por cada uno de los procesos de la organización y posteriormente se relaciona cada escenario con la información, los servicios y los procedimientos de gestión que son usados dentro de los procesos y que deberían verse afectados, para materializar dichos riesgos identificados.

El modelo establece tres tipos de activos a identificar y los subdivide según su naturaleza y propósito con el fin que la valoración del impacto sea hecha por cada uno de estos subgrupos, identificando el efecto causado a la organización la pérdida de la confidencialidad, integridad y disponibilidad de dichos activos.

La ventaja que presenta este modelo es la capacidad de asociación que brinda el hecho que se establezca la relación directa que tienen los diferentes tipos de activos sobre cada situación de riesgo identificada, lo que facilita su valoración y la orienta a que se vea reflejada la importancia que tiene para el negocio cada uno de los activos.

Sin embargo dentro de la catalogación de activos, no se discriminan independientemente los activos tipo hardware, personas, aplicaciones, software, sino que todos los relacionan con los servicios con los que cuenta la organización, lo cual puede hacer perder la visibilidad del impacto que pueda representar la falla sobre alguno de estos elementos a los servicios, en el caso que estos recursos sean compartidos.

Este hecho aunque simplifica la implementación de controles, ya que se determinan los mismos por el grupo de activos, puede hacer que sean implementados controles innecesarios sobre activos que de forma independiente no representen mayor riesgo pero por su agrupación, hereden valores de impacto que alguno de los activos que componen dicho grupo si puedan tener.

La agrupación de activos es válida en la medida que todos los miembros de dicho grupo o su gran mayoría representen situaciones de riesgo con impactos similares, por lo que hacer la desagregación de los componentes de hardware, software, instalaciones físicas y personas, y su evaluación independiente del impacto generado por situaciones de pérdida de confidencialidad, integridad y disponibilidad brindar mayor visibilidad del riesgo potencial al que estaría expuesto la organización.

NIST está orientado al análisis de la clasificación que se le debe dar a la información en sí, más no a los activos que la soportan, por lo que su alcance no considera los activos tipo hardware, software, personas y demás diferentes a la información y los servicios.

La ventaja de este modelo es que hace una clasificación general de la información, teniendo en cuenta los impactos generados por la pérdida de confidencialidad, integridad y disponibilidad de forma independiente.

BIBLIOGRAFÍA

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS. Méthode harmonisée d'analyse des risques. MEHARI 2010. París : CLUSIF, 2010. 26 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 (31, diciembre, 2008). por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la Información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios y la proveniente de terceros países y se dictan otras disposiciones. Bogotá: El Congreso, 2008. 17 p.

CONSEJO SUPERIOR DE ADMINISTRACION ELECTRÓNICA. . Metodología de análisis y gestión de riesgos de los sistemas de información. MARGERIT V2. Madrid : CSAE, 2006. 154 p.

INTERNATIONAL STANDARD ORGANIZATION. Information technology -Security techniques -Information security management systems -Requirements. ISO/IEC 27001:2005. 1 ed. Geneve, Suiza: ISO, 2005. 34 p.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide for mapping types of information and informations Systems to security categories. NIST SP 800-60. Gaithersburg, Estados Unidos : NIST, 2008. 53 p.

--------. Guide to protecting the confidentiality of personally identifiable information. NIST SP 800-122. Gaithersburg, Estados Unidos : NIST, 2010. 59 p.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO, Directrices de la OECD para la seguridad de sistemas y redes de información. Paris : OECD, 2002. 12 p.

FORMATO DE CLASIFICACIÓN DE ACTIVOS BASADO EN LA NORMA ISO 27001 PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ESCALA DE MEDICIÓN	
Mínimo	1
Bajo	2
Medio	3
Alto	4
Muy Alto	5

PONDERACIÓN PROPIEDADES	
Confidencialidad	33%
Integridad	33%
Disponibilidad	33%

ASPECTOS ORGANIZACIONALES	
Operación	33%
Economía	33%
Cumplimiento	33%

ATRIBUTOS DEL ACTIVO					VALORACIÓN				CLASIFICACIÓN	
Nombre Activo	**Tipo de activo**	**Ubicación**	**Propietario**	**Custodio**	**Propiedad**	**Operación**	**Economía**	**Cumplimiento**	**Clasificación Propiedad**	**Clasificación del activo**
SAP	Software	Servidor SAP	Líder Tecnología	Analista de aplicaciones	Confidencialidad	Mínimo	Alto	Bajo	Bajo	Medio
					Integridad	Medio	Mínimo	Muy Alto	Medio	
					Disponibilidad	Bajo	Muy Alto	Mínimo	Medio	
Servidor SAP					Confidencialidad	Alto	Alto	Bajo	Medio	Medio
					Integridad	Medio	Mínimo	Muy Alto	Medio	
					Disponibilidad	Bajo	Muy Alto	Mínimo	Medio	
					Confidencialidad	Mínimo	Alto	Bajo	Bajo	Medio
					Integridad	Medio	Mínimo	Muy Alto	Medio	
					Disponibilidad	Bajo	Muy Alto	Mínimo	Medio	
					Confidencialidad	Mínimo	Alto	Bajo	Bajo	Medio
					Integridad	Medio	Mínimo	Muy Alto	Medio	
					Disponibilidad	Bajo	Muy Alto	Mínimo	Medio	
					Confidencialidad	Mínimo	Alto	Bajo	Bajo	Medio
					Integridad	Medio	Mínimo	Muy Alto	Medio	
					Disponibilidad	Bajo	Muy Alto	Mínimo	Medio	