

Identificación de Activos Críticos de Información

Superintendencia de Transporte — Barranquilla, Atlántico

Documento técnico elaborado para fortalecer los procesos de gestión de riesgos, seguridad de la información, continuidad operativa y disponibilidad de los servicios tecnológicos institucionales.

Información del Documento

Autor: Virgilio Salgado Escorce

Fecha: 04/Marzo/2026

Estructura del Documento:

01	02	03
Introducción	Objetivos	Marco Teórico y Normativo
Contexto de la transformación digital y la gestión de activos de información.	Objetivo general y objetivos específicos del proceso de identificación.	Fundamentos conceptuales, estándares internacionales y normativa aplicable.
04	05	
Identificación y Clasificación de Activos	Auditoría y Conclusiones	
Catálogo de activos tecnológicos y clasificación por nivel de criticidad.	Importancia de la auditoría periódica y conclusiones institucionales.	

1. Introducción

En el contexto de la transformación digital y la creciente dependencia de las tecnologías de la información, las organizaciones requieren identificar, clasificar y gestionar adecuadamente sus activos tecnológicos y de información. Los activos de información constituyen elementos fundamentales para la operación institucional, ya que soportan procesos misionales, administrativos, académicos y financieros.

La identificación de activos críticos permite reconocer aquellos recursos cuya afectación podría comprometer la confidencialidad, integridad y disponibilidad de la información, generando impactos operativos, legales, financieros o reputacionales para la organización.

En este sentido, el presente documento tiene como finalidad establecer el proceso de identificación de activos críticos asociados a la infraestructura tecnológica y a los sistemas de información, con base en el análisis del catálogo institucional de activos tecnológicos y plataformas digitales.

Asimismo, este documento busca fortalecer las prácticas de gestión de seguridad de la información, permitiendo priorizar controles, auditorías y mecanismos de monitoreo que reduzcan los riesgos asociados a fallas técnicas, indisponibilidad de servicios o incidentes de ciberseguridad.

La adecuada identificación de activos críticos constituye un insumo fundamental para la implementación de modelos de gestión como el Sistema de Gestión de Seguridad de la Información (SGSI), alineado con estándares internacionales y con las políticas institucionales de gobierno digital.

2. Objetivo General

Identificar y clasificar los activos críticos de información asociados a la infraestructura tecnológica y los sistemas de información institucionales, con el fin de fortalecer los procesos de gestión de riesgos, seguridad de la información, continuidad operativa y disponibilidad de los servicios tecnológicos.

3. Objetivos Específicos

1

Identificar Activos

Identificar los activos tecnológicos y sistemas de información que soportan los procesos institucionales.

2

Determinar Criticidad

Determinar cuáles activos presentan mayor nivel de criticidad en función de su impacto en la operación.

3

Establecer Criterios

Establecer criterios para la priorización de auditorías, monitoreo y controles de seguridad.

4

Apoyar la Gestión

Apoyar la gestión de riesgos tecnológicos mediante la clasificación de activos críticos y no críticos.

5

Promover Vigilancia

Promover la implementación de mecanismos de vigilancia continua para garantizar la disponibilidad y estabilidad de los servicios tecnológicos.

4. Activos de Información

Un activo de información es cualquier recurso que tiene valor para la organización y que participa en el procesamiento, almacenamiento o transmisión de información. Estos activos pueden incluir:



Sistemas de información



Aplicaciones institucionales



Servidores



Plataformas tecnológicas



Bases de datos



Infraestructura tecnológica



Equipos de red

La gestión adecuada de estos activos permite proteger los pilares fundamentales de la seguridad de la información:

Pilares de la Seguridad de la Información

Confidencialidad

Garantiza que la información solo sea accesible para personas autorizadas.

Integridad

Asegura que la información no sea modificada de forma indebida o no autorizada.

Disponibilidad

Permite que los sistemas y servicios estén disponibles cuando los usuarios los necesiten.

Activos Críticos

Los activos críticos son aquellos cuya afectación puede generar impactos significativos en la operación institucional, tales como:

Interrupción de servicios tecnológicos

Pérdida de información sensible

Afectación a procesos institucionales

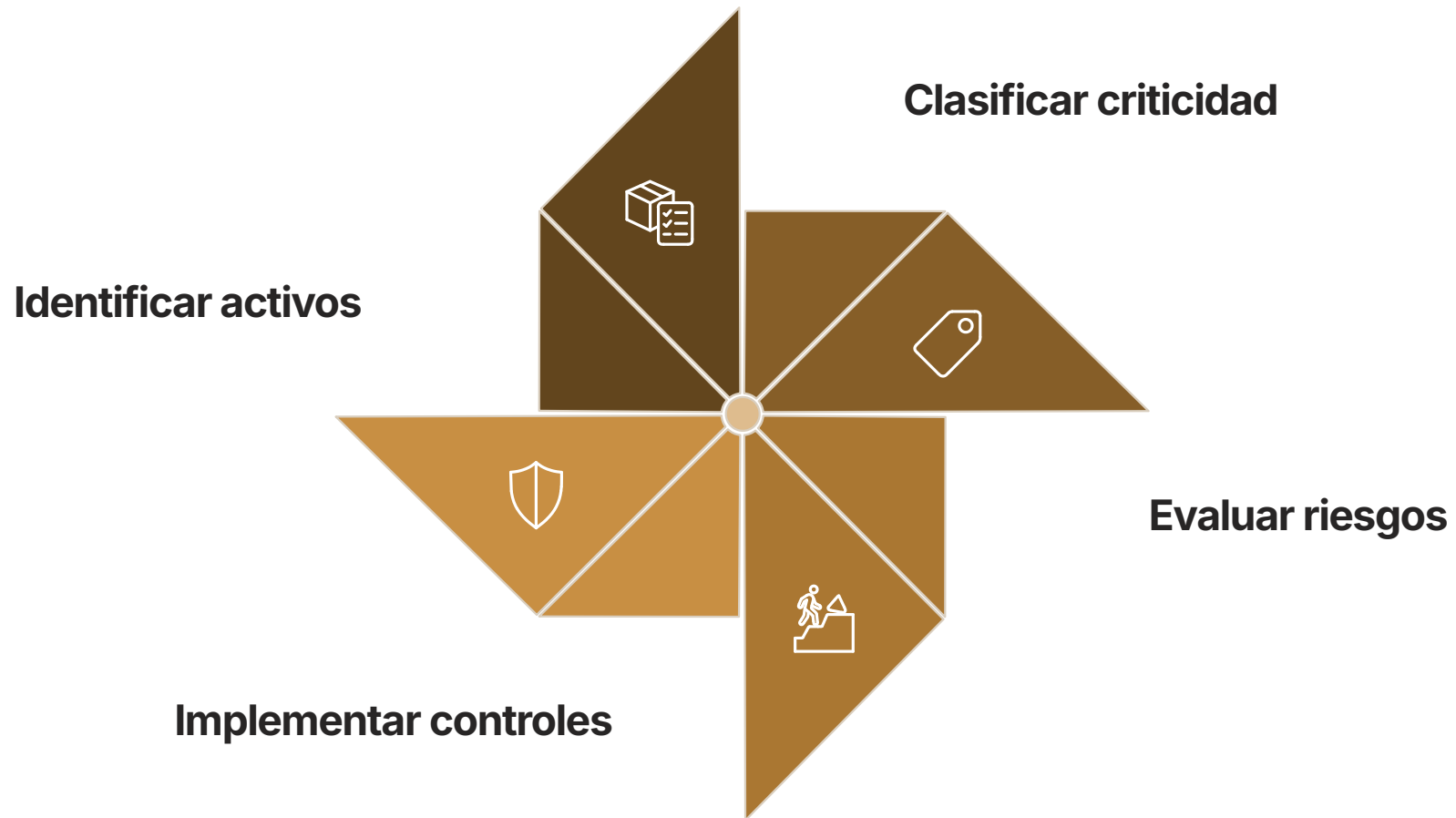
Impacto reputacional

Incumplimiento de obligaciones legales

Estos activos requieren mayores controles de seguridad, monitoreo permanente y auditorías periódicas.

Gestión de Activos de Información

La gestión de activos implica un conjunto de actividades orientadas a fortalecer la postura de seguridad de la organización y garantizar la continuidad operativa.



Este proceso permite fortalecer la postura de seguridad de la organización y garantizar la continuidad operativa.

5. Marco Normativo y Legal

El proceso de identificación, clasificación y gestión de activos críticos de información se encuentra alineado con diferentes marcos normativos, estándares internacionales y disposiciones legales vigentes, los cuales establecen lineamientos para la protección de la información, la gestión de riesgos tecnológicos, la continuidad de los servicios digitales y la implementación de controles de seguridad.

Estos marcos permiten garantizar que la organización adopte buenas prácticas en materia de seguridad de la información, gestión de activos tecnológicos, protección de datos y resiliencia operativa, asegurando que los activos tecnológicos institucionales sean administrados de forma adecuada y bajo criterios de riesgo.

A continuación, se describen los principales estándares y normativas que soportan el presente documento.

ISO/IEC 27001

La norma ISO/IEC 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI).

Este estándar proporciona un marco estructurado para la identificación de activos de información, la evaluación de riesgos y la implementación de controles de seguridad que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

Dentro de los controles establecidos por esta norma se incluye la gestión de activos de información, la cual exige que las organizaciones identifiquen, inventarién y clasifiquen los activos críticos que soportan sus procesos institucionales.

Asimismo, la norma establece que las organizaciones deben implementar mecanismos de monitoreo, auditoría y mejora continua para garantizar que los activos tecnológicos se encuentren protegidos frente a amenazas internas o externas.

ISO/IEC 27002

La norma ISO/IEC 27002 complementa la ISO 27001 proporcionando un conjunto de buenas prácticas y controles de seguridad de la información, los cuales sirven como guía para la implementación de medidas técnicas, organizativas y administrativas.

Este estándar aborda aspectos fundamentales como:



Gestión de activos



Control de accesos



Seguridad de redes



Gestión de incidentes de seguridad



Protección contra malware



Seguridad en operaciones tecnológicas



Monitoreo de sistemas



Continuidad del negocio

Dentro de este marco, la identificación de activos críticos permite establecer controles diferenciados según el nivel de importancia de cada activo dentro de la organización.

6. Identificación de Activos Tecnológicos

Con base en los catálogos institucionales de infraestructura tecnológica y sistemas de información, se identifican diferentes tipos de activos dentro de la organización. Cada uno de estos activos cumple un rol fundamental dentro de los procesos institucionales.

Infraestructura Tecnológica

- Servidores institucionales
- Equipos de red
- Sistemas de almacenamiento
- Infraestructura de virtualización
- Equipos de seguridad perimetral
- Infraestructura de respaldo

Sistemas de Información

- Sistemas administrativos
- Plataformas académicas
- Sistemas financieros
- Sistemas de gestión documental
- Sistemas de autenticación y control de acceso
- Aplicaciones institucionales

7. Clasificación de Activos Críticos

Con base en el análisis del Catálogo de Infraestructura Tecnológica y el Catálogo de Sistemas de Información institucional, se realizó la clasificación de los activos tecnológicos según su nivel de criticidad dentro de la operación institucional.

La clasificación se realizó teniendo en cuenta criterios como:



A partir de estos criterios, los activos se clasifican en tres niveles de criticidad: alta, media y baja.



7.1 Activos de Criticidad Alta (Activos Críticos)

Los activos clasificados como críticos corresponden a aquellos que soportan directamente la operación institucional, los procesos misionales, los servicios tecnológicos centrales y la gestión de la información institucional.

La indisponibilidad de estos activos puede generar:

Interrupción de servicios institucionales

Afectación de procesos administrativos o misionales

Pérdida de información crítica

Impacto reputacional y operativo

Dentro de los activos críticos identificados se encuentran principalmente infraestructura de servidores, plataformas institucionales y sistemas de gestión central.

Sistemas de Información Críticos Identificados

Entre los sistemas institucionales que presentan mayor nivel de criticidad se destacan:



ORFEO ARGON GPL

Sistema de gestión documental institucional utilizado para la administración de comunicaciones oficiales, radicación de documentos y trazabilidad de procesos administrativos.



DYNAMICS

Plataforma utilizada para la gestión administrativa y financiera, la cual soporta procesos organizacionales esenciales.



GLPI (Servicio TI)

Sistema utilizado para la gestión de servicios tecnológicos, incidentes, solicitudes de soporte y administración de activos tecnológicos.

Sistemas de Información Críticos Identificados (Continuación)



Supervisión Inteligente

Plataforma que soporta procesos de análisis, supervisión y gestión de información institucional.



CONNECTA

Sistema utilizado para la integración de procesos y gestión de información entre diferentes áreas institucionales.



CHATBOT /SUPERTRANSPORTE

Plataforma de interacción digital con ciudadanos y usuarios institucionales.



Estos sistemas soportan directamente procesos institucionales y por lo tanto requieren disponibilidad permanente.

Infraestructura Tecnológica Crítica

Dentro del catálogo de infraestructura tecnológica se identifican como activos críticos:

Activo	Descripción
Clusters de virtualización VxRAIL 570F (Hyperconvergencia)	Infraestructura encargada de soportar múltiples máquinas virtuales institucionales.
Switches Dell S4112F-ON (Infraestructura de hiperconvergencia)	Equipos de red que soportan la conectividad del entorno de virtualización.
Chasis Dell M1000e (Cluster físico)	Infraestructura que soporta servidores blade utilizados para ejecutar servicios institucionales.
Servidores Dell PowerEdge	Equipos que alojan aplicaciones institucionales y bases de datos.

La indisponibilidad de estos activos puede afectar simultáneamente múltiples servicios tecnológicos.

Controles Requeridos para Activos Críticos

Debido a su alto nivel de importancia, estos activos deben:



Ser monitoreados permanentemente



Contar con auditorías periódicas



Tener mecanismos de respaldo y recuperación



Implementar planes de continuidad del negocio



Tener controles de seguridad reforzados



Ser incluidos en procesos de gestión de vulnerabilidades

7.2 Activos de Criticidad Media

Los activos clasificados con criticidad media corresponden a aquellos que soportan procesos administrativos o de apoyo institucional. Si bien su indisponibilidad no paraliza completamente la operación institucional, sí puede generar retrasos o afectaciones en algunos servicios.

Entre estos activos se identifican principalmente sistemas especializados utilizados por áreas específicas.

Sistemas de criticidad media identificados

Dentro del catálogo institucional se destacan los siguientes:

Sistema	Descripción
BIBLIOTECA JURÍDICA	Sistema utilizado para la consulta de normativa, jurisprudencia y documentación legal.
CALCULADORA DE DERECHOS	Herramienta de apoyo para el cálculo de valores asociados a trámites institucionales.
DIGITURNO	Sistema utilizado para la gestión de turnos de atención al usuario.
NOTIPRO	Plataforma utilizada para procesos de notificación institucional.
MATRIZ DE INVESTIGACIONES	Sistema de apoyo para la gestión de procesos investigativos.
ORGANISMOS DE APOYO (Tarifas)	Sistema relacionado con gestión de información tarifaria.

Estos sistemas son importantes para el funcionamiento institucional, pero su indisponibilidad no compromete completamente la operación.

Controles Requeridos - Criticidad Media

Los activos de criticidad media deben:

Ser monitoreados regularmente

Contar con respaldos periódicos

Tener control de accesos

Ser incluidos dentro del proceso de gestión de vulnerabilidades

7.3 Activos de Criticidad Baja

Los activos clasificados con criticidad baja corresponden a sistemas o componentes tecnológicos que no afectan directamente la continuidad operativa institucional.

Sin embargo, estos activos no deben ser ignorados dentro del esquema de seguridad, ya que en muchos casos pueden convertirse en vectores indirectos de ataque.

- ❏ Los atacantes frecuentemente explotan sistemas menos protegidos para acceder posteriormente a sistemas críticos.

Activos de criticidad baja identificados

- Aplicaciones secundarias o de apoyo
- Sistemas utilizados temporalmente
- Herramientas auxiliares de análisis
- Estaciones de trabajo
- Componentes de red secundarios
- Sistemas experimentales o en fase de pruebas
- Fuentes Externas (Temporadas Altas)
- Sistemas auxiliares de consulta
- Herramientas de apoyo interno

Controles Requeridos - Criticidad Baja

Aunque estos activos tengan menor impacto, deben:

Mantenerse inventariados

Ser monitoreados dentro del sistema de seguridad

Tener controles mínimos de acceso

Ser incluidos en procesos de actualización y parcheo

Esto permite reducir la probabilidad de que estos sistemas sean utilizados como puntos de entrada para ataques cibernéticos.

8. Importancia de la Auditoría Periódica de Activos Críticos

La auditoría periódica de activos críticos es un elemento fundamental dentro de la gestión de seguridad de la información.

Los activos tecnológicos críticos deben ser auditados de manera constante con el objetivo de:



Detectar vulnerabilidades

Identificar debilidades en la infraestructura antes de que sean explotadas.



Identificar fallas técnicas

Reconocer fallas técnicas que puedan comprometer la operación.



Prevenir interrupciones del servicio

Garantizar la continuidad y disponibilidad de los servicios institucionales.



Fortalecer los controles de seguridad

Mejorar continuamente los mecanismos de protección institucional.

Vigilancia Integral de Activos

El monitoreo continuo permite identificar anomalías, fallos en la infraestructura o posibles incidentes de seguridad antes de que generen impactos significativos en la operación institucional.

Es importante resaltar que los activos no críticos también deben ser monitoreados, ya que muchas veces los atacantes utilizan sistemas secundarios o menos protegidos como puertas de entrada para comprometer sistemas principales.

Por lo tanto, todos los activos tecnológicos deben formar parte de un esquema integral de vigilancia, monitoreo y gestión de riesgos.

9. Conclusiones

La identificación de activos críticos constituye un proceso esencial para fortalecer la seguridad de la información y garantizar la continuidad de los servicios tecnológicos dentro de la organización.

A través del análisis de los catálogos de infraestructura tecnológica y sistemas de información, es posible identificar aquellos activos cuya afectación podría generar impactos significativos en la operación institucional.

Los activos clasificados como críticos deben ser objeto de monitoreo constante, auditorías periódicas y controles de seguridad reforzados, con el fin de prevenir fallas técnicas, indisponibilidad de servicios o incidentes de seguridad.

No obstante, es importante reconocer que incluso los activos con menor nivel de criticidad pueden convertirse en vectores de ataque si no se gestionan adecuadamente. Por esta razón, todos los activos tecnológicos deben integrarse dentro de un esquema de vigilancia permanente que permita detectar riesgos y mitigar vulnerabilidades.

La implementación de procesos de auditoría continua, gestión de riesgos y monitoreo de infraestructura tecnológica permitirá fortalecer la postura de seguridad de la organización y garantizar la protección de la información institucional.