



Implementación de infraestructura de tecnologías de la información y las comunicaciones.

## Criterios de manejo de incidentes en el centro de datos, según la normatividad vigente y estándares

## Criterios de manejo de incidentes en el centro de datos, según la normatividad vigente y estándares

Antes de comenzar a definir los criterios, se deben reconocer términos propios de esta temática:

- **Incidencia:** corresponde a un suceso, eventualidad o novedad que se presenta en un sistema informático, por ejemplo, la caída de un servicio, fallas en el Internet, pérdida de fluido eléctrico, entre otros.
- **Impacto:** hace referencia a la manera como afecta la incidencia al sistema de manera directa, a mayor criticidad mayor será el nivel de impacto, por ejemplo, se puede diferenciar claramente el impacto cuando en un terminal a un usuario deja de funcionarle el mouse o cuando falla el servidor y no se puede ofrecer atención en una ventanilla al público, a mayor complejidad con el sistema o grado de “responsabilidad” el impacto será más elevado.
- **Tiempo de respuesta:** son los tiempos en minutos u horas que se establecen para la prestación de un servicio según el nivel de prioridad y el impacto que se presente. A mayor nivel de impacto al sistema general, menor será el tiempo de respuesta en el servicio.
- **Nivel de criticidad:** permite parametrizar dentro de categorías, la manera en la que un incidente puede ocasionar “ruido” dentro del sistema de información, mientras más alto sea el grado de compromiso del incidente con el sistema, más alta será su “calificación” y por tanto su tiempo de respuesta deberá corresponder según lo establecido como parámetro organizacional.

Los criterios de manejo de incidentes en el centro de datos se pueden dividir de la misma manera en la que se reciben los servicios en una mesa de ayuda o help desk, por tanto, se realizará una clasificación según su importancia y grado de afectación al sistema. MinTic ha diseñado como ejemplo las tablas Nivel de Criticidad de Impacto y Tiempos de respuesta según los incidentes, las cuales se describen a continuación en la Tabla 1 y Tabla 2.

**Tabla 1**

**Niveles de Criticidad de Impacto. Fuente MinTIC.**

Nivel de Criticidad	Valor	Definición
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0,25	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	0,50	Sistemas que apoyan más de una dependencia o proceso de la entidad.
Alto	0,75	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1,00	Sistemas Críticos.

Nota. Elaboración del experto 2022

**Tabla 2.**

**Tiempos Máximos de Atención de Incidentes. Fuente MinTIC.**

Nivel Prioridad	Tiempo de Respuesta
Inferior	3 horas
Bajo	1 hora
Medio	30 minutos
Alto	15 minutos
Superior	5 minutos

Nota. Elaboración del experto 2022.



Para conocer más sobre el manejo de incidentes se puede consultar como referencia la Guía para la gestión y clasificación de incidentes de seguridad de la información.

**MinTIC (2022)**

[https://www.mintic.gov.co/gestionti/615/articles-5482\\_G21\\_Gestion\\_Incidentes.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf)

Nota. Elaboración del experto 2022