PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

¿Qué se considera un incidente?

- Robo o pérdida de equipos.
- Acceso no autorizado.
- Virus o malware.
- Suplantación de identidad.
- Eliminación accidental de información.
- Ataques informáticos.
- Divulgación no autorizada de información.
- Falla de servidores.
- Caída de servicios críticos.

Procedimiento

1. Detección
Cualquier funcionario que identifique un incidente deberá reportarlo inmediatamente al Área de Sistemas.

2. Registro
El Área de Sistemas documentará el incidente, indicando fecha, hora, descripción, sistemas afectados y acciones iniciales.

3. Contención
Se adoptarán medidas para limitar el impacto del incidente y proteger la información institucional.

4. Recuperación
Se restablecerán los servicios afectados utilizando los mecanismos de recuperación disponibles.

5. Cierre
Se documentarán las causas, las acciones implementadas y las recomendaciones para evitar la recurrencia del incidente.