**Integrantes:** Azuero Xavier **Nivel:** Tercero

Anchundia Bryan **Modalidad:** Semipresencial

Itaz Lenin **Jornada:** Sábado

Nagua Cristian **Código:** 19191

**Carrera:** Informática

**Docente:** Ing. Cristhian Cola

**Tema:** Tecnologías de la información (GitHub)

# **Estructura de tecnología**

Esta sección contiene información sobre la estructura y funcionamiento del Servicio de Informática, quiénes forman las distintas áreas, etc.

* **Servicio de Tecnologías de la Información y las Comunicaciones (STIC)**
  + **Área de Sistemas y Atención al Usuario**
    - **Configuración de Sistemas**
    - **Servicios de Gestión**
    - **Microinformática**
  + **Área de Apoyo a la Docencia**
  + **Área de Desarrollo**
    - **Sistemas de Información de Gestión Académica**
    - **Sistemas de Información de Gestión Administrativa**
    - **Web Institucional**
  + **Área de Comunicaciones**
    - **Infraestructura de Red**
    - **Telefonía**

**Área de Sistemas y Atención al Usuario**

Contribuye a la misión del STIC mediante el apoyo a la selección, mantenimiento e implantación de servidores centrales, sistemas operativos, sistemas de seguridad y soporte de bases de datos.

* Configuración de Sistemas
* Servicios de Gestión
* Microinformática

**Área de Apoyo a la Docencia**

Esta área tiene como función principal la instalación, configuración, mantenimiento y gestión de la infraestructura necesaria para el desarrollo de prácticas informáticas de las asignaturas, tanto de enseñanzas regladas como no regladas. También se encarga de la gestión de las aulas de informática de libre acceso para alumnos, de las salas de usuarios de apoyo a la investigación y a la gestión administrativa para PDI y PAS.

**Área de Desarrollo**

Es la encargada del desarrollo, implantación, y mantenimiento de las aplicaciones informáticas que dan soporte a la gestión administrativa en la Universidad de Almería.

* Sistemas de Información de Gestión Académica
* Sistemas de Información de Gestión Administrativa
* Web Institucional

**Área de Comunicaciones**

Tiene como objetivo proporcionar una potente herramienta de trabajo a los usuarios de la UAL: una red de comunicaciones rápida, fácil de usar, segura y sobre la que se pueda acceder al mayor número posible de servicios en Internet y en la propia UAL.

* Infraestructura de Red
* Telefonía

**Análisis de Riesgo TIC**

La provisión de servicios TIC pasa por el correcto funcionamiento de una serie de activos, cada uno de ellos con su función específica. Si alguno de estos activos se ve comprometido por la materialización de una determinada amenaza, el propio servicio se verá afectado. Para determinar el nivel de riesgo real de una entidad hay que realizar un análisis de riesgo.

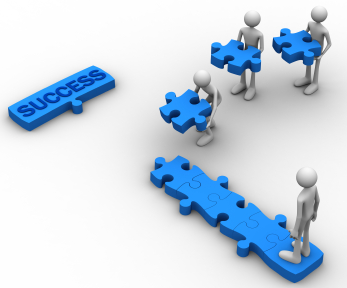
La primera actividad a realizar en un análisis de riesgos es identificar cuáles son los activos que soportan los sistemas de información de la organización.

Un activo es cualquier elemento que tenga valor para la entidad, desde un PC concreto, a un recurso de red o una persona física necesaria para el desarrollo de una actividad.

Con el objetivo de estructurar la información de forma coherente, los activos han de estar clasificados en función de su naturaleza, intentado usar un modelo por capas. Esto permitirá clasificar los sistemas diferenciando la funcionalidad de los activos entre sí, y además facilitará próximos pasos, como definir sus dependencias.

El análisis puede empezar a estructurarse según necesidades específicas, los activos pueden ser des del tipo proceso de negocio, pasando por el personal que trabaja y hasta una ubicación física.

Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a una empresa u organización, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles. Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo.



FODA

**FORTALEZAS**

1.Disposición de recursos económicos para fortalecer los sistemas de información.

2. Contar con software operativo en últimas versiones.

3. Todos los funcionarios de la entidad tienen acceso a la tecnología, facilitando el uso de funciones cooperativas y conjuntas.

4. Disposición de la administración para responder a cambios tecnológicos.

5. Apoyo de la administración en la capacitación especializada de los funcionarios del área.

6. Disposición al cambio por parte del personal de TI.

7. Orientación de la Entidad a procesos, mediante la implementación del Sistema de Gestión de Calidad

**OPORTUNIDADES**

1.Normatividad y Estándares emanadas por MINTIC y MEN.

2. La creación de nuevos productos por la tendencia del mercado.

3. Disponibilidad de arquitecturas informáticas estándar del mercado, como SOA (Service Oriented Architecture), BPM (Business Process Management), CMS (Content Management Systems) y DW (Data Warehouse).

4. Nuevas tendencias en la operación y administración de recursos informáticos.

5. Restructurar administrativamente el área de TI

6. La ampliación de cobertura y accesibilidad de las redes de comunicación, lo que permiten mayor acercamiento a las IES.

7. La integración de los proyectos de Tecnología dentro del Marco de la Normatividad de seguridad de la información.

8. Uso de nuevas tecnologías, por la naturaleza de FODESEP.

9. El uso del software libre permite ahorro de recursos y optimización del presupuesto

**DEBILIDADES**

1.Concentración del conocimiento en algunos funcionarios.

2. Documentación deficiente o desactualizada.

3. Monitoreo insuficiente de procesos, dispositivos y equipos.

4. Existencia de bases de datos y aplicativos en diferentes equipos sin control del área de tecnología.

5. Capacitación a usuarios finales para apropiar herramientas tecnológicas.

6. Falta capacitación y concienciación al personal en los beneficios del uso de nuevas tecnologías.

7. Falta de identificación de procesos existe cadena valor y actualización de la misma.

8. Pocas posibilidades de crecimiento personal.

9. No contar con las herramientas (software) necesarias para la buena administración del área.

10. Ser vista TI como un área de soporte y mantenimiento de equipos. pero en la misión dices que eres un área de soporte

11. Riesgo de pérdida de memoria institucional en sistemas por cambio tecnológicos.

12. No utilización de herramientas existentes por falta de conocimiento de éstas.

13. Falta de trabajo en equipo de las áreas usuarias con el Área de Sistemas.

14. Fuga de información, por falta de controles.

**AMENAZAS**

1.Altos costos de la tecnología.

2. Cambio de lineamientos en las políticas tecnológicas Gubernamentales.

3. Riesgo de seguridad en la sede, que pueda ocasionar inversiones no planeadas,

4. Monopolios de la tecnología

5. Redes de comunicaciones externas inestables.

6. Ataques a la infraestructura informática

7. Inadecuados controles de acceso lógicos y físicos

8. Regulación desfavorable

9. Falta de compromiso real frente a los proyectos de vinculación de tecnología

BIBLIOGRAFÍA

<https://www.fodesep.gov.co/images/docs/Tecnologia/PLAN%20ESTRAT%C3%89GICO%20DE%20TECNOLOG%C3%8DAS%20DE%20LA%20INFORMACI%C3%93N%20-PETI%202016-2019.pdf>