# Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Trabajo de Final de Máster

Autor: Andrea Maricela Plaza Cordero

Director: Antonio José Segovia Henares

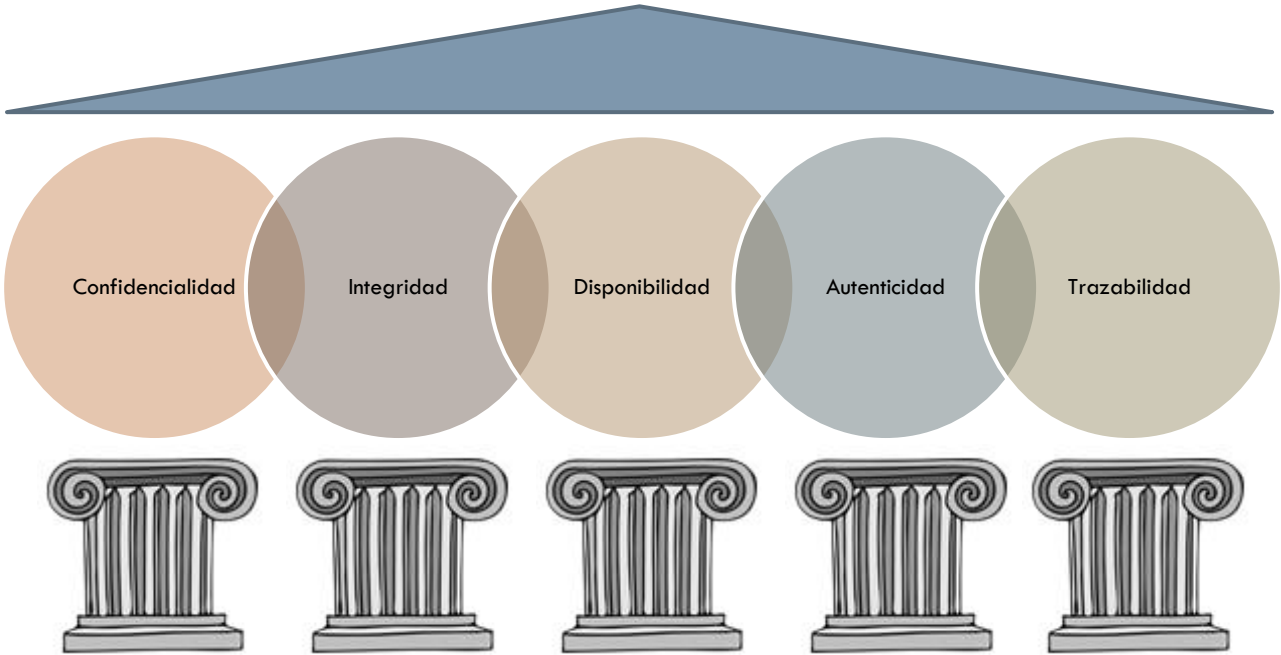
## Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013 en la IES

# Seguridad de la Información

- **Información hoy en día es uno de los principales activos en toda organización.**

- **Seguridad de la información:** Se ocupa de proteger la información en todas sus formas y en cualquier momento de su ciclo de vida ante cualquier amenaza que pueda generar pérdida o disminución de su valor.

# Dimensiones de la Seguridad de la Información



# Implementación del SGSI: Reseña Histórica

- Antes de aparecer la LOES las Instituciones de Educación Superior manejaban la información sin control de ninguna organización.

- Después la LOES solicita diversa información a las Instituciones de Educación Superior bajo la premisa:
  - Educación Superior = Bien Público

# Implementación del SGSI: Reseña Histórica

- Organismos de control:
  - CES (Consejo de Educación Superior)
    - "…Planificar, regular y coordinar el Sistema de Educación Superior, y la relación entre sus distintos actores con la Función Ejecutiva y la sociedad ecuatoriana; para así garantizar a toda la ciudadanía una Educación Superior de calidad que contribuya al crecimiento del país"
  - CEAACES (Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior)
    - "Ejercer la rectoría de la política pública para el aseguramiento de la calidad de la educación superior del Ecuador a través de procesos de evaluación, acreditación y categorización en las IES"

# Implementación del SGSI: Antecedentes

- Situación de la IES:
  - Propuestas Ad-hoc que son iniciativa de los Coordinadores de las áreas y/o Departamentos.
  - Poca documentación y la que se tiene no posee un estándar.
  - No existen criterios de seguridad de la información definidos por el Consejo Superior.
  - El personal no posee concienciación sobre la importancia de la información.

# Implementación del SGSI: Normativa de Referencia

- ISO/IEC 27001:2013 -> Especificaciones para la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI).
  - Requerimientos:

- ISO/IEC 27002:2013 -> Es el código de buenas prácticas en la gestión de la seguridad de la información.
  - Dominios:
  - Controles:

# 1. Situación Actual

- Identificar la situación actual que la IES atraviesa en base al Análisis Diferencial.
- Establecer los objetivos y el alcance del Plan de Implementación del SGSI.

# 1. **Situación actual:** Contextualización

- La empresa seleccionada es una Institución de Educación Superior cofinanciada.
- La IES está ubicada en Ecuador teniendo su matriz en la ciudad de Cuenca y sede en Quito.
- Posee 21 años de vida institucional mediante la Ley de Creación en el Registro Oficial de la República del Ecuador.
- Al momento alberga aproximadamente 22453 estudiantes entre el nivel de grado y posgrado matriculados en este periodo, y 1780 empleados entre administrativos y docentes.

# Seguridad de la Información: Información de la IES

- Proyectos
- Planes Analíticos
- Acta de Grado
- Record Académico
- Calificaciones
- Planes de Seguimiento
- Etc.

**Académica**

- Balances
- Presupuestos
- Cuentas
- Costos
- Etc.

**Financiera**

- Contratos
- Sueldos
- Datos personales del personal
- Nómina
- Etc.

**Recursos Humanos**

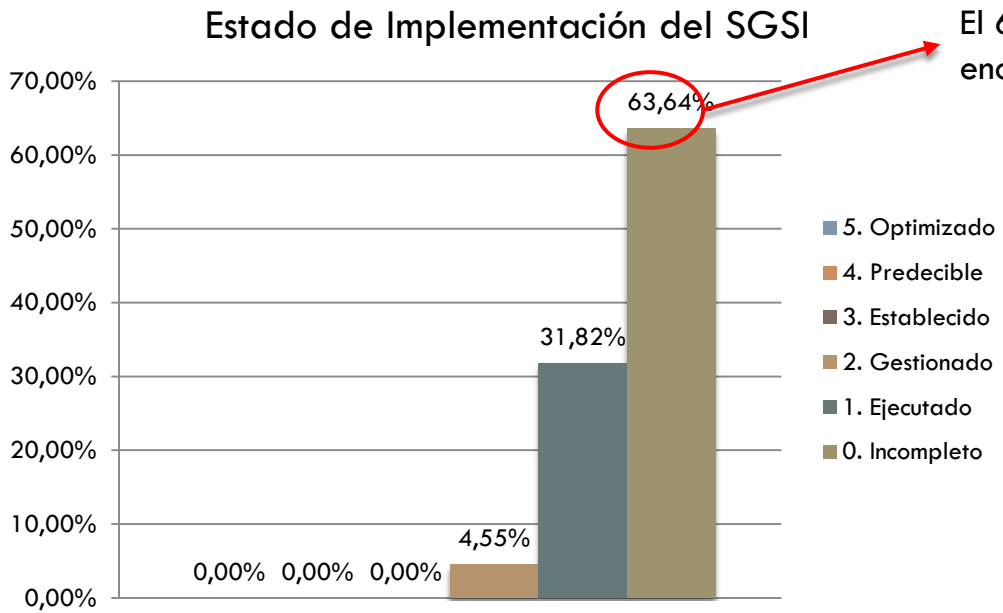
# 1. **Situación actual:** Análisis Diferencial

- El análisis diferencial (GAP Analysis) permite conocer el estado general de la IES en relación a la seguridad de la información permitiendo definir el alcance.
- Análisis de los controles implantados en la IES vs controles necesarios según la norma ISO 27001:2013 e ISO/IEC 27002:2013, dando como resultado el análisis de la madurez de los controles hasta el momento implementados.

# 1. **Situación actual:** Análisis Diferencial

| Nivel | Descripción |
|---|---|
| 5. Optimizado | El proceso predecible es mejorado de forma continua. |
| 4. Predecible | El proceso predecible se encuentra en ejecución dentro de los límites definidos. |
| 3. Establecido | El proceso gestionado se encuentre implementado mediante un proceso definido. |
| 2. Gestionado | El proceso ejecutado se encuentra implementado mediante una gestión (planificado, supervisado y ajustado) y los resultados se encuentran establecidos, controlados y mantenidos adecuadamente. |
| 1. Ejecutado | El proceso implementado alcanza su propósito. |
| 0. Incompleto | El proceso no se encuentra implementado o no alcanza el propósito definido. Además existe muy poca o ninguna evidencia de haberse presentado un logro sistemático del propósito del proceso. |

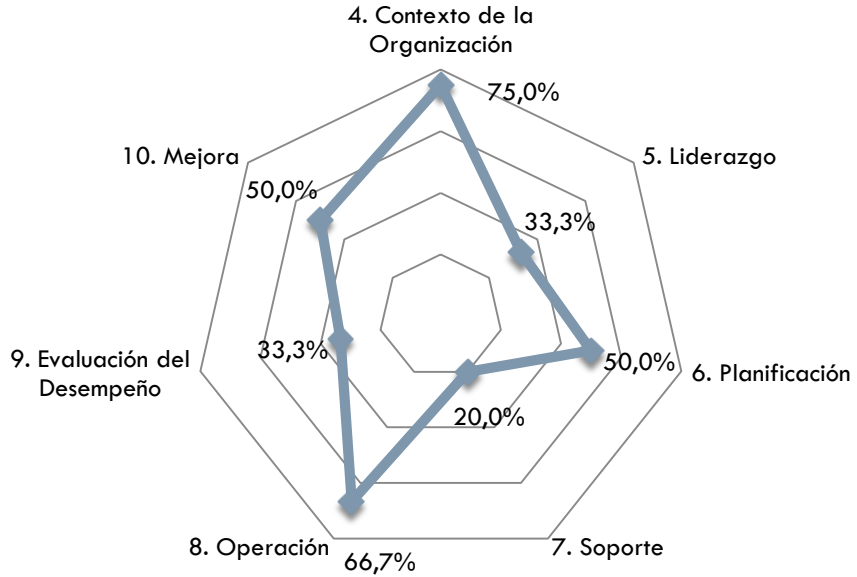
# 1. **Situación actual:** Análisis Diferencial




El 63.64% de requerimientos no se encuentran implementados

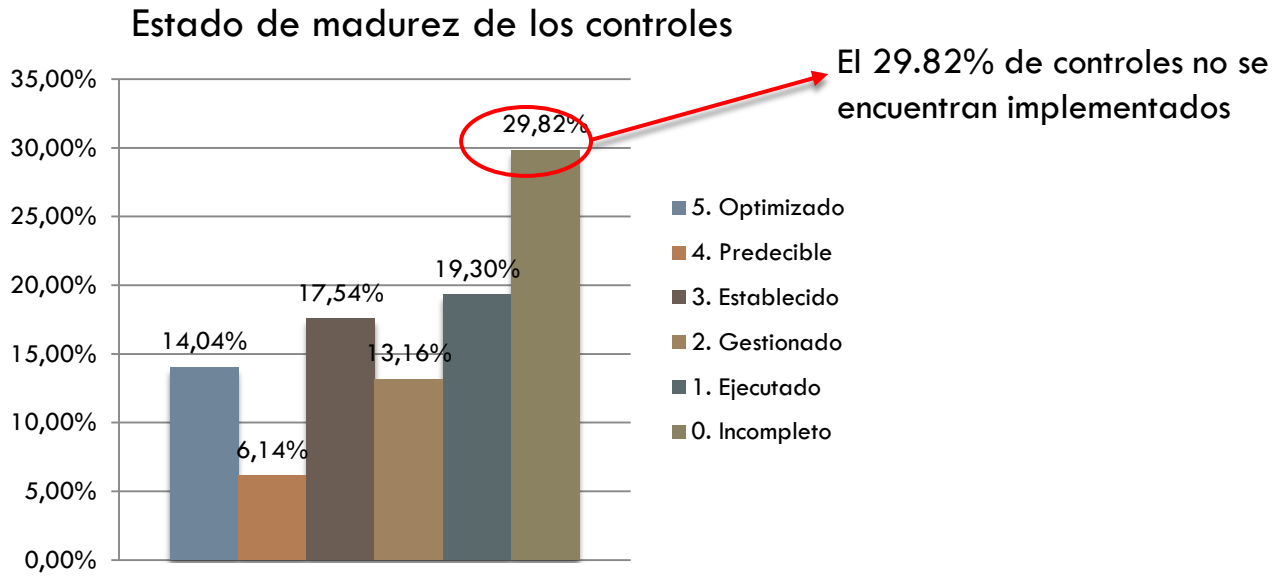
# 1. **Situación actual:** Análisis Diferencial

Estado de implementación
ISO/IEC 27001:2013



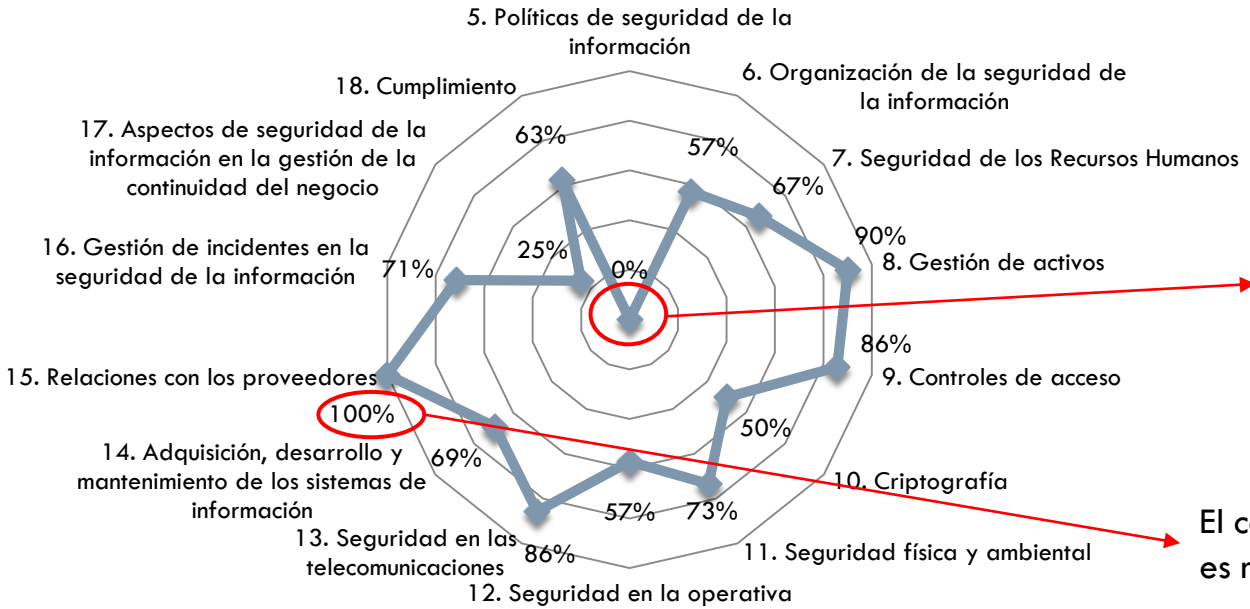

Todo requerimiento posee un nivel de implementación.

# 1. **Situación actual:** Análisis Diferencial



# 1. **Situación actual:** Análisis Diferencial

## Estado de implementación ISO/IEC 27002:2013




No se ha establecido una Política de Seguridad

El control posee un proceso que es mejorado continuamente

# 1. **Situación actual:** Alcance del SGSI

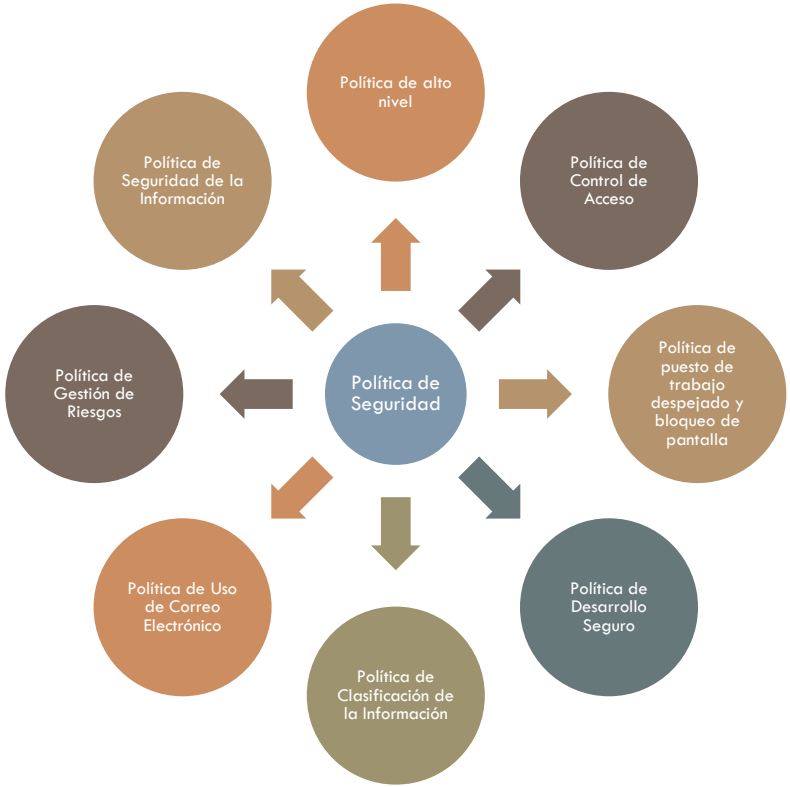
La implementación se va a realizar en la matriz de la IES, que se encuentra ubicada en la ciudad de Cuenca, bajo el siguiente escenario:

- La gestión de la seguridad de la información de la IES que cubre los sistemas de información Académicos, Financieros y de Recursos Humanos, la red de comunicación LAN, la seguridad en las telecomunicaciones, la parte física y ambiental y los equipos para procesamiento de datos según la declaración de aplicabilidad versión 2.
- Se va a excluir el Ambiente Virtual de Aprendizaje, los equipos y dispositivos móviles, la red LAN, los computadores de administrativos y docentes, y de los laboratorios, infraestructura y redes de la sede Quito.

# 2. Sistema de Gestión Documental

- Definir la documentación básica para implementar el Sistema de Gestión de Seguridad de la Información según la norma ISO 27001.
- Disponer de una normativa común de seguridad que regule como la IES va a trabajar en materia de seguridad de la información

# 2. Sistema de Gestión Documental: Esquema Documental



# 2. Sistema de Gestión Documental: Esquema Documental

# 2. Sistema de Gestión Documental: Declaración de Aplicabilidad

- Por cada control se procedió a indicar si aplica o no, con su respectiva justificación

| Objetivo | Control | Estado | Justificación |
|---|---|---|---|
| **5. Políticas de seguridad de la información** | | | |
| 5.1 Dirección de gestión de seguridad de la información | 5.1.1 Políticas de seguridad de la información | SI | La IES debe poseer un conjunto de políticas de seguridad de la información aprobadas por el Consejo Superior y comunicadas según corresponda. |
| | 5.1.2 Revisión de las políticas de seguridad de la información | SI | Las políticas de seguridad de la información deben ser evaluadas anualmente y someterlas a aprobación por el Comité de Seguridad y posterior el Consejo Superior. |
| **6. Organización de la seguridad de la información** | | | |
| 6.2 Los dispositivos móviles y el teleworking | 6.2.1 Política de dispositivo móvil | SI | Se deben incorporar políticas para gestionar el riesgo de manejar dispositivos móviles para acceder a información de la IES. |
| | 6.2.2 Teleworking | NO | En base al alcance el análisis es a nivel de la matriz y no con la sede de Quito. |

# 3. Análisis de Riesgos

- Identificación de los riesgos, su magnitud y las áreas que requieren medidas de protección.

- FASES de la Metodología de Análisis de Riesgos.
  1. Inventario de Activos
  2. Valoración de Activos
  3. Análisis de Amenazas
  4. Impacto Potencial y Nivel de Riesgo Aceptable

# 3. Análisis de Riesgos: Metodología MAGERIT

- No es una medida de seguridad
- Permite identificar los peligros a los que se encuentra expuesta la IES



- ¿Qué hay que proteger?
- ¿De qué o quién hay que proteger, y por qué?
- ¿Cómo nos vamos a proteger?

- Metodología: MAGERIT
  - Elaborado por el Ministerio de Administraciones Públicas.
  - Puede ser aplicada en cualquier organización.
  - El resultado se expresa en valores económicos
    - Las decisiones estarán fundamentadas y serán fácilmente defendible.
  - Aplicación es costosa.

# 3. Análisis de Riesgos: Inventario de Activos

| Caracterización | Cantidad |
|---|---|
| [D] Datos/Información | 8 |
| [K] Claves criptográficas | 1 |
| [S] Servicio | 13 |
| [SW] Software | 7 |
| [HW] Hardware | 9 |
| [COM] Redes de Comunicaciones | 3 |
| [Media] Soportes de Información | 4 |
| [AUX] Equipamiento auxiliar | 2 |
| [L] Instalaciones | 3 |
| [P] Personal | 8 |

58 activos

Listar todos los recursos según el alcance del SGSI que presentan valor a la IES y por lo tanto deben ser protegidos ante amenazas

La gestión de la seguridad de la información de la IES que cubre los sistemas de información Académicos, Financieros y de Recursos Humanos, la red de comunicación LAN, la seguridad en las telecomunicaciones, la parte física y ambiental, los equipos para procesamiento de datos según la declaración de aplicabilidad versión 2.

# 3. Análisis de Riesgos: Inventario de Activos

Activo

Caracterización

| Código | Denominación | Descripción | Propietario |
|---|---|---|---|
| | | **[D] Datos/Información** | |
| D-001 | Información académica | Datos de los estudiantes, proyectos, investigaciones, notas, etc. | Vicerrector Académico |
| D-002 | Información financiera | Datos sobre balances, prepuestos, cuentas, costos, etc. | Secretario Técnico de Finanzas |
| D-003 | Información del personal | Datos sobre contratos, sueldos, datos personales de los empleados (docentes y administrativos), nóminas, etc. | Secretario Técnico de Recursos Humanos |
| D-005 | Datos del Sistema Académico, Financiero y de Recursos Humanos | Base de Datos Oracle Standard Edition 11g, que almacena los datos académicos, financieros y del personal. | Administrador de Base de Datos |
| | | **[S] Servicio** | |
| S-001 | Sistema Académico | Sistema que se encarga de controlar todo lo académico para el nivel de Grado y Posgrado como son: las inscripciones, matrículas, proyectos, resoluciones, calificaciones, académicos, paracadémicos, evaluación docente, entre otros. | Vicerrector Académico |
| S-002 | Sistema Financiero | Sistema que se encarga de controlar todo lo referente a la contabilidad de la IES como son: balances, presupuestos, cuentas, costos, activos fijos, adquisiciones, facturación, flujo de caja, entre otros. | Secretario Técnico de Finanzas |
| S-003 | Sistema de Recursos Humanos | Sistema que se encarga de controlar todo lo referente al personal de la IES como son: contratos, sueldos, datos personales de los empleados, nóminas, entre otros. | Secretario Técnico de Recursos Humanos |
| | | **[COM] Redes de Comunicaciones** | |
| COM-002 | LAN | Se refiere a las configuraciones para permitir conectividad en la matriz Cuenca como son: creación de VLANs, configuraciones, entre otros. | Administrador de Redes |
| | | **[L] Instalaciones** | |
| L-001 | Matriz Cuenca | Está instalación corresponde a las aulas, laboratorios, oficinas administrativas y de investigación. | Vicerrector de Sede |
| L-002 | Rectorado | Este edificio posee las oficinas administrativas. | Vicerrector General |
| L-003 | Departamento TIC | Centro de procesamiento de datos de la matriz Cuenca. | Director del Departamento de Tecnologías de Información y Comunicación |
| | | **[P] Personal** | |
| P-001 | Alta Dirección | Está conformado por: Vicerrector General, Vicerrector de Sede, Vicerrector Académico, Coordinadores Académicos de Sede y las distintas Secretarías. | Rector |
| P-002 | Director del Departamento de TIC | Es el Director del Departamento de Tecnologías de Información y Comunicación | Alta Dirección |

# 3. **Análisis de Riesgos:** Valoración de Activos

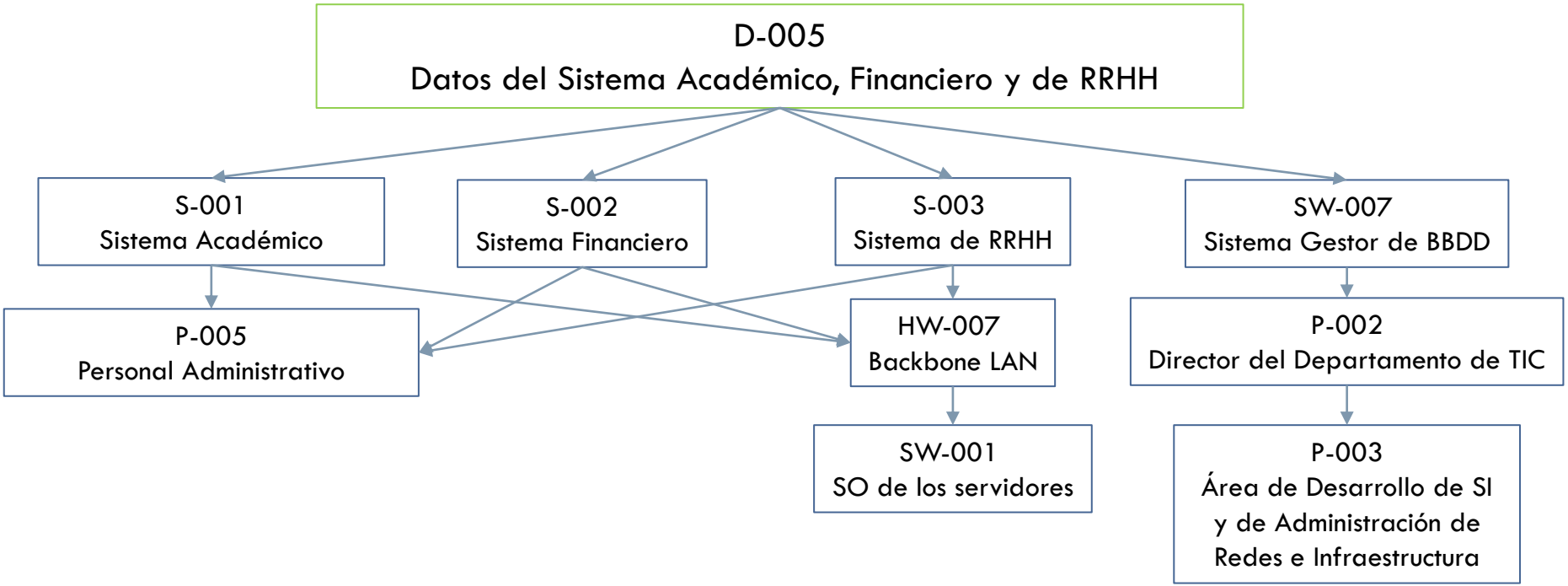
- **Dependencia de los Activos:** Los activos se encuentran jerarquizados

- Los que se encuentran en la parte superior son los dependientes de los que se encuentran en el nivel inferior, por lo tanto ante la presencia de una amenaza en el activo inferior tendrá como consecuencia un daño sobre el activo superior por la presencia de la dependencia.

- [D] Datos/Información
  - D-001 Información Académica.
  - D-002 Información Financiera.
  - D-003 Información del Personal
  - D-005 Datos del Sistema Académico, Financiero y de Recursos Humanos.
- [S] Servicios
  - S-001 Sistema Académico

Activos considerados de nivel "Muy Alto" de los activos esenciales

# 3. **Análisis de Riesgos:** Dependencia de los Activos



# 3. **Análisis de Riesgos:** Dimensiones de Seguridad

- **Valor de Reposición**
  - Valor de reposición en caso de que no se tenga el activo.
- **Valor de configuración**
  - Valor desde que se compra el activo hasta que se configure y esté listo para su uso.
- **Valor de uso del activo**
  - Valor que pierde durante el tiempo que no se puede utilizar el activo para la función que desempeña dentro de los procesos.
- **Valor de pérdida de oportunidad**
  - Valor que pierde la Empresa por no disponer del activo

| Valor | Criterio |
|---|---|
| 10 | Daño muy grave a la IES |
| 7 - 9 | Daño grave a la IES |
| 4 - 6 | Daño importante a la IES |
| 1 - 3 | Daño menor a la IES |
| 0 | Irrelevante para la IES |

# 3. Análisis de Riesgos: Dimensiones de Seguridad

| Valor | Criterio |
|---|---|
| 10 | Daño muy grave a la IES |
| 7 - 9 | Daño grave a la IES |
| 4 - 6 | Daño importante a la IES |
| 1 - 3 | Daño menor a la IES |
| 0 | Irrelevante para la IES |

| Código | Denominación | | | Dimensiones | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | Disponibilidad | Integridad | Confidencialidad | Autenticidad | Trazabilidad |
| **[D] Datos/Información** | | | | | | | | |
| D-001 | Información académica | $ 200.000,00 | Muy Alto | 6 | 9 | 4 | 2 | 4 |
| D-002 | Información | $ 200.000,00 | Muy Alto | 5 | 9 | 7 | 2 | 4 |
| D-003 | Información | $ 200.000,00 | Muy Alto | 4 | 8 | 6 | 2 | 4 |
| D-005 | Datos del S | $ 200.000,00 | Muy Alto | 8 | 9 | 6 | 6 | 3 |
| | | | | | | | | |
| S-001 | Sistema Ac | $ 200.000,00 | Muy Alto | 9 | 6 | 6 | 9 | 9 |
| S-002 | Sistema Fi | $ 200.000,00 | Muy Alto | 5 | 6 | 6 | 9 | 9 |
| S-003 | Sistema de | $ 40.000,00 | Medio | 5 | 5 | 5 | 8 | 7 |

**Valoración de Activos**

| Nivel | Abreviatura | Rango | Valor |
|---|---|---|---|
| Muy Alto | MA | valor > 100000 $ | $200.000,00 |
| Alto | A | 50000 $ < valor > 100000 $ | $ 75.000,00 |
| Medio | M | 10000 $ < valor > 50000 $ | $ 40.000,00 |
| Bajo | B | 5000 $ < valor > 15000 $ | $ 10.000,00 |
| Muy Bajo | MB | valor < 5000 $ | $ 5.000,00 |

# 3. **Análisis de Riesgos:** Análisis de Amenazas

Para el análisis de las amenazas se va a usar el Libro 2 “Catálogo de Elementos” de la metodología MAGERIT, el mismo que clasifica en los siguientes grupos:

- Desastres naturales.
- De origen industrial
- Errores y fallos no intencionados.
- Ataques intencionados.

# 3. Análisis de Riesgos: Análisis de Amenazas

| Análisis de Amenazas | | Tipo de Activo | | |
|---|---|---|---|---|
| | | [D] Datos / Información | | |
| Código | Amenazas | D-001 | $ 200.000,00 | |
| **[N] Desastres naturales** | | | | |
| [N.1] | Fuego | | | |
| [N.2] | Daños por agua | | | |
| [N.*] | Desastres naturales | | | |
| **[I] De origen industrial** | | | | |
| [L.1] | Fuego | | | |
| [I.2] | Daños por agua | | | |
| [I.11] | Emanaciones electromagnéticas | | | |
| **[E] Errores y fallos no intencionados** | | | | |
| [E.1] | Errores de los usuarios | [D] 40%<br>[I] 70%<br>[C] 40%<br>[A] 0%<br>[T] 0% | 0,005479<br>$ 767,06 | 70% |
| **[A] Ataques intencionados** | | | | |
| [A.5] | Suplantación de la identidad del usuario | [D] 0%<br>[I] 70%<br>[C] 40%<br>[A] 90%<br>[T] 0% | 0,00274<br>$ 493,20 | 90% |
| [A.6] | Abuso de privilegios de acceso | [D] 30%<br>[I] 60%<br>[C] 20%<br>[A] 0%<br>[T] 0% | 0,005479<br>$ 657,48 | 60% |
| [A.30] | Ingeniería social | | | |
| | | $ 5.424,72 | | |

**Frecuencia**

| Descripción | Abreviatura | Rango | Valor |
|---|---|---|---|
| Frecuencia muy alta | MA | 1 vez al día | 365 / 365 = 1 |
| Frecuencia alta | A | 1 vez cada 2 semanas | (52/2) / 365 = 0,071233 |
| Frecuencia media | M | 1 vez cada mes | (12/1) / 365 = 0,032877 |
| Frecuencia baja | B | 1 vez cada 6 meses | (12/6) / 365 = 0,005479 |
| Frecuencia muy baja | MB | 1 vez cada 12 meses | (12/12) / 365 = 0,002740 |

**Riesgo intrínseco:** Situación en la que nos encontramos teniendo en consideración todos los elementos que posee la IES.

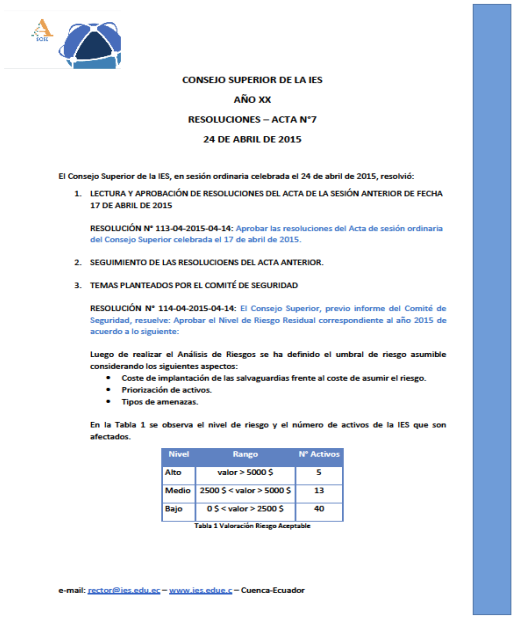
Valor del activo * Vulnerabilidad * Impacto

# 3. Análisis de Riesgos: Propietario del Riesgo

**Propietario de los Riesgos**
"Persona o entidad con responsabilidad y autoridad para gestionar un riesgo"

| Código | Amenazas | [D] Datos/Información | [K] Claves Criptográficas | [S] Servicio | [SW] Software | [HW] Hardware |
|---|---|---|---|---|---|---|
| | | | | | | **[N] Desastres naturales** |
| [N.1] | Fuego | | | | | Coordinador del Departamento de Salud Ocupacional |
| [N.2] | Daños por agua | | | | | Coordinador del Departamento de Salud Ocupacional |
| [N.*] | Desastres naturales | | | | | Coordinador del Departamento de Salud Ocupacional |
| | | | | | | **[I] De origen industrial** |
| [L.1] | Fuego | | | | | Coordinador del Departamento de Salud Ocupacional |
| [I.2] | Daños por agua | | | | | Coordinador del Departamento de Salud Ocupacional |
| | | | | | | **[E] Errores y fallos no intencionados** |
| [E.1] | Errores de los usuarios | Responsable de Seguridad de la Información | Responsable de Seguridad de la Información | Responsable de Seguridad de la Información | Responsable de Seguridad de la Información | |
| [E.2] | Errores del administrador | Responsable de Seguridad de la Información | Responsable de Seguridad de la Información | Director del Departamento de Tecnologías de la Información | Director del Departamento de Tecnologías de la Información | Director del Departamento de Tecnologías de la Información |
| [E.3] | Errores de monitorización (log) | Director del Departamento de Tecnologías de la Información | | | | |
| [E.4] | Errores de configuración | Director del Departamento de Tecnologías de la Información | | | | |
| | | | | | | **[A] Ataques intencionados** |
| [A.3] | Manipulación de registros de actividad (log) | Director del Departamento de Tecnologías de la Información | | | | |
| [A.4] | Manipulación de la configuración | Director del Departamento de Tecnologías de la Información | | | | |
| [A.5] | Suplantación de la identidad del usuario | Director del Departamento de Tecnologías de la Información | Director del Departamento de Tecnologías de la Información | Director del Departamento de Tecnologías de la Información | Director del Departamento de Tecnologías de la Información | |

# 3. Análisis de Riesgos: Aprobación por parte de la Dirección



**CONSEJO SUPERIOR DE LA IES**

**AÑO XX**

**RESOLUCIONES – ACTA N°7**

**24 DE ABRIL DE 2015**

El Consejo Superior de la IES, en sesión ordinaria celebrada el 24 de abril de 2015, resolvió:

1. LECTURA Y APROBACIÓN DE RESOLUCIONES DEL ACTA DE LA SESIÓN ANTERIOR DE FECHA 17 DE ABRIL DE 2015

   RESOLUCIÓN N° 113-04-2015-04-14: Aprobar las resoluciones del Acta de sesión ordinaria del Consejo Superior celebrada el 17 de abril de 2015.

2. SEGUIMIENTO DE LAS RESOLUCIOENS DEL ACTA ANTERIOR.

3. TEMAS PLANTEADOS POR EL COMITÉ DE SEGURIDAD

   RESOLUCIÓN N° 114-04-2015-04-14: El Consejo Superior, previo informe del Comité de Seguridad, resuelve: Aprobar el Nivel de Riesgo Residual correspondiente al año 2015 de acuerdo a lo siguiente:

   Luego de realizar el Análisis de Riesgos se ha definido el umbral de riesgo asumible considerando los siguientes aspectos:

   - Coste de implantación de las salvaguardias frente al coste de asumir el riesgo.
   - Priorización de activos.
   - Tipos de amenazas.

   En la Tabla 1 se observa el nivel de riesgo y el número de activos de la IES que son afectados.

| Nivel | Rango | N° Activos |
|---|---|---|
| Alto | valor > 5000 $ | 5 |
| Medio | 2500 $ < valor > 5000 $ | 13 |
| Bajo | 0 $ < valor > 2500 $ | 40 |

Tabla 1 Valoración Riesgo Aceptable

e-mail: rector@ies.edu.ec – www.ies.edue.c – Cuenca-Ecuador

RESOLUCIÓN N° 114-04-2015-04-14: El Consejo Superior, previo informe del Comité de Seguridad, resuelve: Aprobar el Nivel de Riesgo Residual correspondiente al año 2015 de acuerdo a lo siguiente:

Luego de realizar el Análisis de Riesgos se ha definido el umbral de riesgo asumible considerando los siguientes aspectos:

- Coste de implantación de las salvaguardias frente al coste de asumir el riesgo.
- Priorización de activos.
- Tipos de amenazas.

En la Tabla 1 se observa el nivel de riesgo y el número de activos de la IES que son afectados.

| Nivel | Rango | N° Activos |
|---|---|---|
| Alto | valor > 5000 $ | 5 |
| Medio | 2500 $ < valor > 5000 $ | 13 |
| Bajo | 0 $ < valor > 2500 $ | 40 |

Tabla 1 Valoración Riesgo Aceptable

# 3. Análisis de Riesgos: Impacto Potencial y Nivel de Riesgo Aceptable

**Nivel de Riesgo**

| Código | Denominación | Valoración Cuantitativa | Valoración Cualitativa |
|---|---|---|---|
| | **[D] Datos/Información** | | |
| D-001 | Información académica | $ 5.424,72 | ALTO |
| D-002 | Información financiera | $ 5.588,98 | ALTO |
| D-003 | Información del personal | $ 2.794,72 | MEDIO |
| D-005 | Datos del Sistema Académico, Financiero y de Recursos Humanos | $ 3.726,34 | MEDIO |
| | **[S] Servicio** | | |
| S-001 | Sistema Académico | $ 11.507,05 | ALTO |
| S-002 | Sistema Financiero | $ 9.452,12 | ALTO |
| S-006 | Portal WEB | $ 3.051,24 | MEDIO |
| S-013 | Servicio de copias de seguridad | $ 2.856,30 | MEDIO |
| | **[SW] Software** | | |
| SW-001 | Sistema Operativo de los servidores | $ 3.308,30 | MEDIO |
| SW-003 | Software Académico | $ 3.760,29 | MEDIO |
| SW-007 | Sistema Gestor de Base de Datos | $ 3.678,26 | MEDIO |
| | **[HW] Hardware** | | |
| HW-001 | Servidores | $ 6.082,77 | ALTO |
| HW-004 | Computadores para docentes | $ 3.786,33 | MEDIO |
| HW-007 | Backbone LAN | $ 3.205,71 | MEDIO |
| | **[COM] Redes de Comunicaciones** | | |
| COM-001 | WIFI | $ 3.643,88 | MEDIO |
| COM-002 | LAN | $ 4.325,32 | MEDIO |
| | **[Media] Soportes de Información** | | |
| Media-002 | Documentos Académicos | $ 4.237,68 | MEDIO |
| | **[L] Instalaciones** | | |
| L-001 | Matriz Cuenca | $ 4.219,37 | MEDIO |

**Valoración de Dimensiones de Seguridad**

| Nivel | Abreviatura | Rango | Valor |
|---|---|---|---|
| Alto | A | valor > 5000 $ | $ 5.000,00 |
| Medio | M | 5000 $ < valor > 2500 $ | $ 2.500,00 |
| Bajo | B | valor < 2500 | $ - |

# 4. Propuesta de Proyectos

- Luego de la planificar se deberá implementar el Plan de gestión de riesgos o Plan de seguridad, es decir implementar los controles adecuados, con los responsables, el presupuesto aprobado, entre otros, con el fin de evitar los daños intrínsecos al factor de riesgo.

# 4. Propuestas de Proyectos

Elaboración y divulgación de las políticas de Seguridad de la Información

Plan de concienciación (capacitación y formación del personal)

Plan de virtualización de servidores

Plan de continuidad

# 4. Propuestas de Proyectos: Proyecto 1

**Elaboración y divulgación de las políticas de Seguridad de la Información:**

- Crear nuevas políticas: Al momento existe un documento donde se encuentran plasmadas siete políticas en materia de seguridad de la información, pero muchas áreas y/o departamentos no presentan una política definida a nivel de la IES.
- Divulgación de las políticas: No se ha difundido de la manera adecuada las políticas existentes.

- Presupuesto: $ 86660, 00
- Tiempo: 56 días laborables

# 4. Propuestas de Proyectos: Proyecto 1

## Elaboración y divulgación de las políticas de Seguridad de la Información

| Políticas definidas | Políticas a desarrollar |
|---|---|
| Política de Alto Nivel | Política de Manejo de Activos |
| Política de Control de Acceso | Política de Divulgación de Información |
| Política de puesto de trabajo despejado y bloque de pantalla | Política de Gestión de Pruebas en el Desarrollo Seguro |
| Política de Desarrollo Seguro | |
| Política de Clasificación de la Información | |
| Política de Uso de Correo Electrónico | |
| Política de Gestión de Incidentes | |

# 4. Propuestas de Proyectos: Proyecto 2

**Plan de Concienciación (capacitación y formal del personal)**

- Capacitación de las políticas de seguridad de la información de la IES.
- Capacitación en la legislación tanto de la IES como el Reglamento de Régimen Académico del CES y la Ley Orgánica de Educación Superior del Ecuador.

- Presupuesto: $ 11675, 00
- Tiempo: 36 días laborables

# 4. Propuestas de Proyectos: Proyecto 2

## Plan de Concienciación (capacitación y formal del personal)

| Capacitaciones | Personal | |
|---|---|---|
| | Administrativo | Académico |
| Capacitación de las políticas de seguridad de la información de la IES | x | x |
| Capacitación del Departamento Financiero | x | |
| Capacitación del Departamento RRHH | x | |
| Capacitación a nivel de legislación Académica | x | x |
| Capacitación en materia de Ingeniería social | x | x |
| Capacitación en el manejo de activos | x | x |

# 4. Propuestas de Proyectos: Proyecto 3

## Plan de Virtualización de Servidores

- Simplificar la gestión de las copias de seguridad y la recuperación ante incidentes.
- Reducir el tiempo de inactividad por actualizaciones y/o mantenimiento.
- Crear un entorno de prueba de forma rápida y fácil que permita validar parches y actualizaciones antes de implementar en el servidor de producción.
- Conseguir el nivel de Gestionado en los controles que presenten un nivel inferior a este, en el dominio 7 Seguridad de los Recursos Humanos.

- Presupuesto: $ 9530, 00
- Tiempo: 43 días laborables

# 4. Propuestas de Proyectos: Proyecto 4

## Plan de Continuidad del Negocio

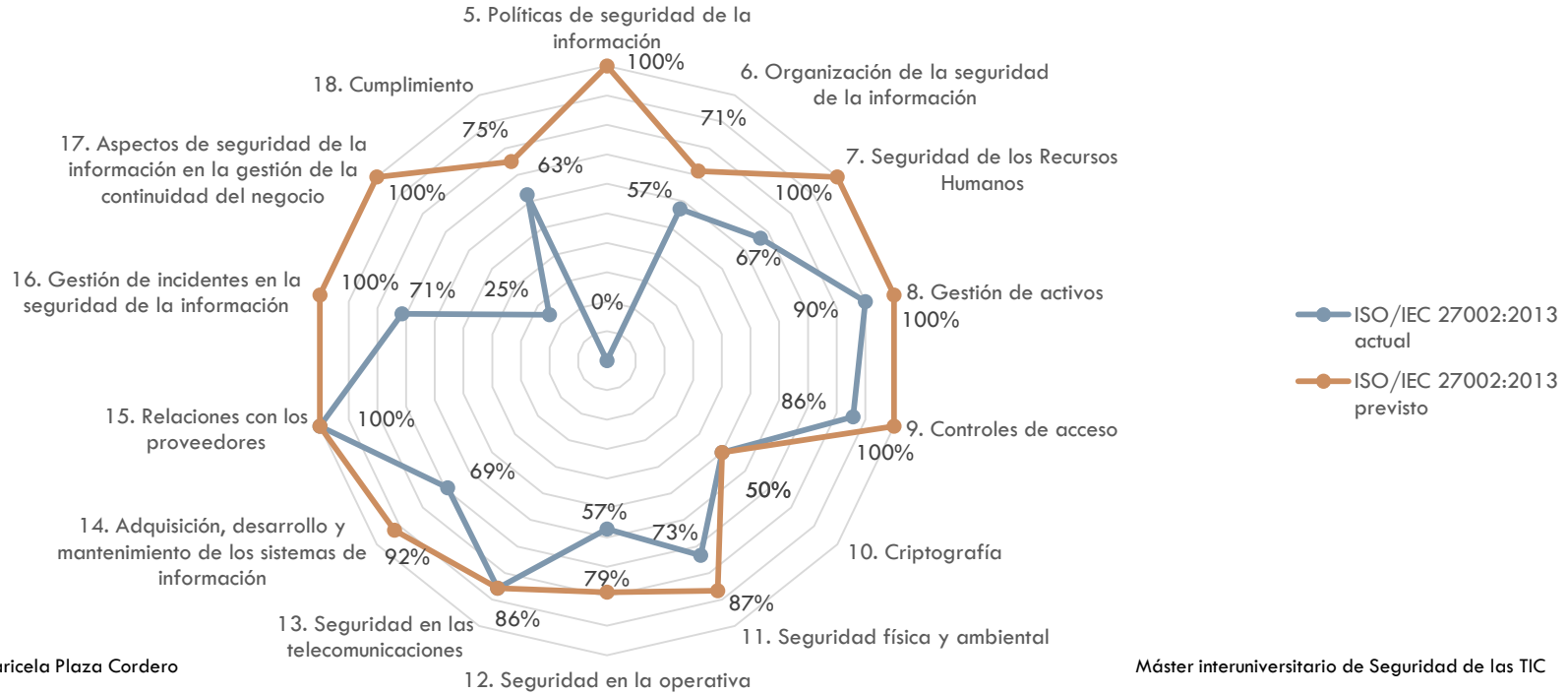
- Brindar una respuesta de forma rápida y ágil a las situaciones que los controles implementados no han podido controlar.
- Conseguir el nivel de Gestionado en los controles que se encuentren en un nivel inferior al mencionado, en el dominio 17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

- Presupuesto: $ 13380, 00
- Tiempo: 51 días laborables

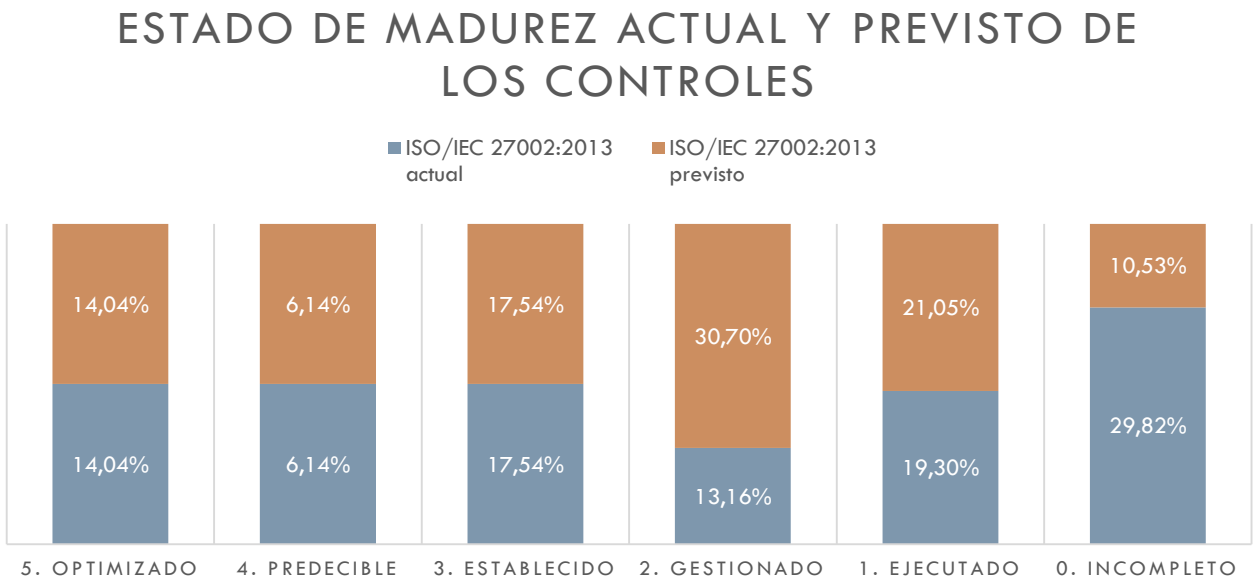
| Descripción | Responsable |
|---|---|
| Plan de continuidad de Desarrollo de Sistemas de Información | Coordinador de Desarrollo de Sistemas de Información |
| Plan de continuidad de Redes e Infraestructura | Coordinador de Administración de Redes e Infraestructura |

# 4. Propuestas de Proyectos

## Estado de madurez actual y previsto de la ISO/IEC 27002:201



# 4. Propuestas de Proyectos



# 5. Auditoría de Cumplimiento

- Objetivo:
  - Revisar y analizar los controles, sistemas, procedimientos y políticas en materia de seguridad informática, a fin de verificar el estado de implementación del Sistema de Gestión de Seguridad de la Información.

# 5. Auditoría de Cumplimiento: Alcance

- La presente auditoría se rige a la verificación del estado de cumplimiento de los controles de seguridad de la norma ISO/IEC 27002:2013 en base a la declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información y las políticas propuestas.

# 5. Auditoría de Cumplimiento: Inventario de las políticas

| Externo |
| --- |
| • Ley Orgánica de Educación Superior.<br>• Reglamento de Régimen Académico del CES.<br>• Reglamento Interno de Régimen Académico de la IES.<br>• Norma ISO/IEC 27001:2013.<br>• Norma ISO/IEC 27002:2013. |

| Interno |
| --- |
| • Política de Seguridad de la Información.<br>• Política de Alto Nivel.<br>• Política de Control de Acceso.<br>• Política de puesto de trabajo despejado y bloqueo de pantalla.<br>• Política de Desarrollo Seguro.<br>• Política de Clasificación de la Información<br>• Política de uso de Correo Electrónico.<br>• Política de Gestión de Incidentes.<br>• Política de Manejo de Activos.<br>• Política de Divulgación de Información.<br>• Política de Gestión de Pruebas en el desarrollo seguro.<br>• Procedimiento de Auditorías Internas.<br>• Procedimiento de Revisión por la Dirección.<br>• Gestión de Indicadores.<br>• Gestión de Roles y Responsabilidades.<br>• Metodología de Análisis de Riesgos.<br>• Declaración de Aplicabilidad.<br>• Plan de concienciación.<br>• Plan de virtualización de servidores.<br>• Plan de elaboración y divulgación de las políticas de SI. |

# 5. **Auditoría de Cumplimiento:** Procedimiento del control de pruebas

- **Gestión de las incidencias.** Si en el transcurso de la auditoría se detecta una vulnerabilidad grave que pueda comprometer la seguridad de la información se procederá de la siguiente manera:
  - Se comunica al Responsable de Seguridad de la Información la incidencia y circunstancias que la provocaron, para que el mismo tome las medidas que considere convenientes.
  - El detalle de la incidencia se documentará en el informe de auditoría.

# 5. **Auditoría de Cumplimiento:** Procedimiento del control de pruebas

- Se considera una vulnerabilidad grave las siguientes situaciones:
  - Una filtración o modificación no autorizada de información considerada como confidencial.
  - Un malfuncionamiento que pueda provocar una denegación de servicio.
  - Un proceso mal ejecutado que pueda provocar problemas legales.
  - Cualquier incidente que pueda ocasionar un estado inoperable

# 5. Auditoría de Cumplimiento: Definición de las pruebas

- **Estrategia de prueba:** Cada CMM por control poseerá un estado, en base al detalle presentado a continuación:

  - Naranja: Control ha superado el estado actual.
  - Verde: Control pose un estado inferior con respecto al estado previsto.
  - Rojo: Control posee un estado inferior a lo indicado en el estado actual.
  - Rosado: Control ha superado el estado previsto.
  - Sin color: Control no ha cambiado su estado

# 5. **Auditoría de Cumplimiento:** Definición de las pruebas

- **Recogida de información:** Los hallazgos se clasifican de la siguiente manera:
  - **No conformidad mayor:** Se incumple completamente con la norma.
  - **No conformidad menor:** Se incumple un punto de un apartado de la política o norma.
  - **Observación:** Es una recomendación, que podría convertirse en No Conformidad, en caso de no ser tratado.
  - **Oportunidad de mejora:** Es sólo una recomendación.

# 5. Auditoría de Cumplimiento: Metodología empleada

| Nivel | Efectividad | Descripción |
|---|---|---|
| L5. Optimizado | 100% | Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos. |
| L4. Gestionado y medible | 95% | Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos.<br>Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia. |
| L3. Proceso definido | 90% | La organización entera participa en el proceso.<br>Los procesos están implantados, documentados y comunicados mediante entrenamiento. |
| L2. Reproducible, pero intuitivo | 50% | Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método.<br>No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo. |
| L1. Inicial / Ad-hoc | 10% | Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal.<br>Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo. |
| L0. Inexistente | 0% | Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver. |
| N/A | N/A | No aplica |

# 5. Auditoría de Cumplimiento: Presentación de Resultados

**No conformidad mayor:** Se incumple completamente con la norma. 5 controles

| Objetivo | | | Control | | | Justificación | |
|---|---|---|---|---|---|---|---|
| 6.2 Los dispositivos móviles y el teleworking | 0% | L0 | 6.2.1 Política de dispositivo móvil | 0% | L0. | Se ha identificado la necesidad de una Política de dispositivo móvil, pero no existe nada definido estrictamente. | **No conformidad mayor:** No existe una Política de dispositivo móvil. |
| **9. Control de acceso [66.6% - L3]** | | | | | | | |
| 9.4 Control de acceso a sistemas y aplicaciones | 52% | L3 | 9.4.3 Gestión de contraseñas de usuario | 10% | L1. | Dentro de la Política de Control de Acceso SGSI_PO_SI_2015-01 se explica la responsabilidad de la gestión de las contraseñas. Internamente cada intervalo de tiempo al empleado dependiendo de su rol, se le solicita la modificación de su contraseña. | **No conformidad mayor:** No existe una política particular o dentro del documento Política de Control de Acceso SGSI_PO_SI_2015-01 una sección específica sobre la gestión de las contraseñas. |
| **10. Criptografía [25% - L2]** | | | | | | | |
| 10.1 Controles criptográficos | 25% | L2 | 10.1.1 Política sobre el uso de controles criptográficos | 0% | L0. | No existe una política sobre el uso de controles criptográficos para la protección de la información | **No conformidad mayor:** No existe una política particular para el uso de controles criptográficos. |
| **11. Seguridad física y ambiental [72.5% - L3]** | | | | | | | |
| 11.2 Seguridad de los equipos | 68.3% | L3 | 11.2.5 Salida de activos fuera de las dependencias de la empresa | 50% | L2. | Existe un conjunto de normas donde se ha definido el procedimiento para la salida de equipos fuera de las dependencias, pero se ha evidenciado que no es una política formal por parte de la IES. | **No conformidad mayor:** Dentro de la Política de manejo de activos no existe una norma o artículo donde se legisle dicho proceso. |
| | | | 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones | 10% | L1. | No existe ninguna política donde se establezca la seguridad cuando los equipos salen de la IES, es un proceso intuitivo. | **No conformidad mayor:** Dentro de la Política de manejo de activos no existe una norma o artículo donde se legisle dicho proceso. |

Inicial: 0. Incompleto
Previsto: 2. Gestionado
Actual: L1. Inicial/Ad-hoc

# 5. Auditoría de Cumplimiento: Presentación de Resultados

**No conformidad menor:** Se incumple un punto de un apartado de la política o norma.

5 controles

| Objetivo | | | Control | | | Justificación | |
|---|---|---|---|---|---|---|---|
| **7. Seguridad de los Recursos Humanos [71.6% - L3]** | | | | | | | |
| 7.2 Durante el empleo | 48.3% | L2 | 7.2.2 Concienciación sobre la seguridad de la información, la educación y la formación | 45% | L2. | Se ha evidenciado que dentro de las propuestas de proyectos se incluye un plan de concienciación con la propuesta de seis capacitaciones. | **No conformidad menor:** Existe el proyecto de cada una de las capacitaciones, pero no se ha contratado a la Empresa Capacitadora. |
| | | | 7.2 | 10% | L1. | En la Reglamento de Procesos Disciplinarios y de Aplicación del Art. 207 de la Ley Orgánica de Educación Superior, de la IES se establecen las sanciones a empleados y estudiantes por infracciones. | **No conformidad menor:** Existe el Reglamento respectivo pero se incumple con el artículo de sanciones graves. |
| **Gestión de activos [73.7% - L3]** | | | | | | | |
| 8.3 Manejo de soportes | 35.3% | L2 | 8.3.1 Gestión de soportes extraíbles | 10% | L1. | Existe el respectivo procedimiento para la gestión de soportes extraíbles en base a su clasificación. | **No conformidad menor:** Se incumple con un punto del procedimiento donde se indica el uso de las plantillas. |
| **11. Seguridad física y ambiental [72.5% - L3]** | | | | | | | |
| 11.1 Áreas seguras | 80% | L3 | 11.1.2 Controles físicos de entrada | 100% | L5. | Se ha evidenciado que dependiendo del área y/o información están implementados controles físicos de entrada como son: tarjetas, controles de vigilancia, geometría de la mano, entre otros. | **No conformidad menor:** Se ha evidenciado que existe problemas con el control de geometría de la mano. |
| **18. Cumplimiento [33.1% - L2]** | | | | | | | |
| 18.1 Cumplimiento de los requisitos legales y contractuales | 32% | L2 | 18.1.4 Protección de datos y privacidad de la información personal | 10% | L1. | Existe una Política para la protección de los datos personales. | **No conformidad menor:** Los empleados no conocen sobre la Política para la Protección de los datos personales. |

Inicial: 0. Incompleto
Previsto: 2. Gestionado
Actual: L2. Reproducible

# 5. Auditoría de Cumplimiento: Presentación de Resultados

**Observación:** Es una recomendación, que podría convertirse en No Conformidad, en caso de no ser tratado.

4 controles

| Objetivo | | | Control | | | Justificación | |
|---|---|---|---|---|---|---|---|
| **5. Políticas de seguridad de la información [ 97.5% - L5 ]** | | | | | | | |
| 5.1 Dirección de gestión de seguridad de la información | 97.5% | L5 | 5.1.2 Revisión de las políticas de seguridad de la información | 95% | L4. | Existe un plan que permitirá la revisión de las políticas. | Observación: Existe un plan de revisión de las políticas de seguridad de la información con su respectiva planificación, pero no se ha ejecutado. |
| **Gestión de activos [73.7% - L3]** | | | | | | | |
| 8.1 Responsabilidad de los activos | 83.8% | L3 | 8. | 50% | L2. | Existe una gestión para el uso y procesamiento de la información y los activos. | **Observación:** Se recomienda actualizar el proceso de gestión para el uso y procesamiento de la información y los activos. |
| **. Control de acceso [66.6% - L3]** | | | | | | | |
| 9.2 Gestión de acceso de usuario | 70.5% | L3 | 9.2.5 Revisión de los derechos de acceso de los usuarios | 88% | L3. | Anualmente los propietarios de los activos entregan un listado de derecho de accesos de los usuarios que tienen a su cargo. | **Observación:** Los listados de acceso a nivel de red no son considerados. |
| **14. Adquisición, desarrollo y mantenimiento de los sistemas de información [68.3% - L3]** | | | | | | | |
| 14.2 Seguridad en los procesos de desarrollo y soporte | 67.5% | L3 | 14.2.2 Procedimientos de control de cambios en los sistemas | 50% | L2. | El procedimiento para el control de cambios se basa en una nomenclatura que define el tipo de cambio, versión, sistema, entre otros datos. No está definido formalmente por la IES. | **Observación:** El Responsable de Seguridad de Información conjuntamente con el Director del Departamento de TIC deberían elevar la propuesta al Consejo Superior para su aprobación. |

Inicial: 0. Incompleto
Previsto: 2. Gestionado
Actual: L4. Gestionado y medible

# 5. Auditoría de Cumplimiento: Presentación de Resultados

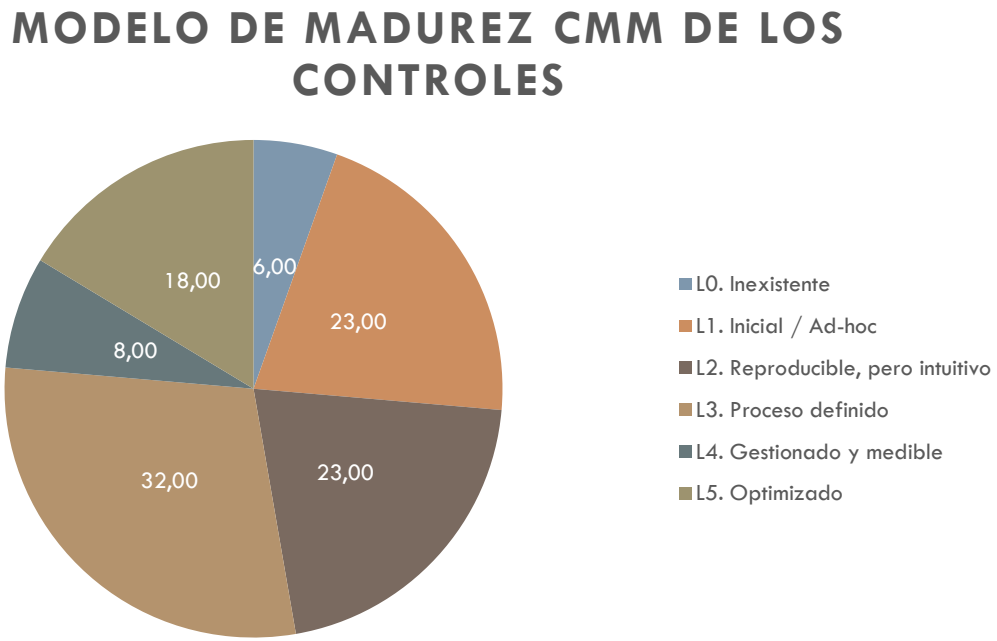
**Oportunidad de mejora:** Es sólo una recomendación.

7 controles

| Objetivo | | | Control | | | Justificación | |
|---|---|---|---|---|---|---|---|
| **7. Seguridad de los Recursos Humanos [71.6% - L3]** | | | | | | | |
| 7.3 Terminación y cambio de empleo | 90% | L3 | 7.3.1 La terminación o el cambio de las responsabilidades laborales | 90% | L3. | El Departamento de Recursos Humanos posee un proceso para la terminación o cambio de responsabilidades, que se encuentra gestionado por el Departamento de TIC. | **Oportunidad de mejora:** Se recomienda que el proceso sea traducido como una política de la IES. |
| **8. Gestión de activos [73.7% - L3]** | | | | | | | |
| 8.2 Clasificación de la información | 98.7% | | | 96% | L5. | El Departamento de Gestión Documental provee del procedimiento de la manipulación de los activos. | **Oportunidad de mejora:** Se recomienda revisión del procedimiento ya que se encuentra alineado al documento SGSI_PO_Si_2015-01 Política de Clasificación de la Información. |
| 8.3 Manejo de soportes | 35.3% | L2 | 8.3.2 Eliminación de los soportes | 46% | L2. | Dentro de la propuesta de proyectos se ha definido la Política de manejo de activos, pero no existe una capacitación formal. | **Oportunidad de mejora:** Se recomienda dentro de la propuesta de proyectos incluir la Capacitación sobre la eliminación de los soportes. |
| **11. Seguridad física y ambiental [72.5% - L3]** | | | | | | | |
| 11.2 Seguridad de los equipos | 68.3% | L3 | 11.2.3 Seguridad del cableado | 90% | L3. | Existen normas establecidas para cableado estructurado, como la norma ANSI/TIA/EIA-568-A, pero no en todos los bloques. | **Oportunidad de mejora:** A pesar de que existen las normas establecidas. No todas las instalaciones cuentan con cableado estructurado. |
| **12. Seguridad en la Operativa [29.3% - L2]** | | | | | | | |
| 12.6 Gestión de la vulnerabilidad técnica | 45% | L2 | 12.6.1 Gestión de las vulnerabilidades técnicas | 0 | L0. | No se ha definido responsable para la gestión de las vulnerabilidades técnicas. | **Oportunidad de mejora:** Se recomienda incluir dentro del documento SGSI_PR_RR_2015-01 al responsable de dicha tarea. |
| **16. Gestión de incidentes en la seguridad de la información [55.7% - L3]** | | | | | | | |
| 16.1 Gestión de incidentes de seguridad de la información y mejoras | 55.7% | L3 | 16.1.5 Respuesta a incidentes de seguridad de la información | 50% | L2. | Los incidentes de seguridad se responden en base a los procedimientos establecidos por la IES. | **Oportunidad de mejora:** A pesar de que existe el proceso establecido no todos los empleados responden en base al procedimiento. |
| **18. Cumplimiento [33.1% - L2]** | | | | | | | |
| 18.1 Cumplimiento de los requisitos legales y contractuales | 32% | L2 | 18.1.2 Derechos de propiedad intelectual (DPI) | 90% | L3. | Se encuentran establecidos los procedimientos que garantizan el derecho de propiedad intelectual y el uso de software privado. | **Oportunidad de mejora:** Se recomienda incluir en el Plan de Concienciación una capacitación sobre propiedad intelectual. |

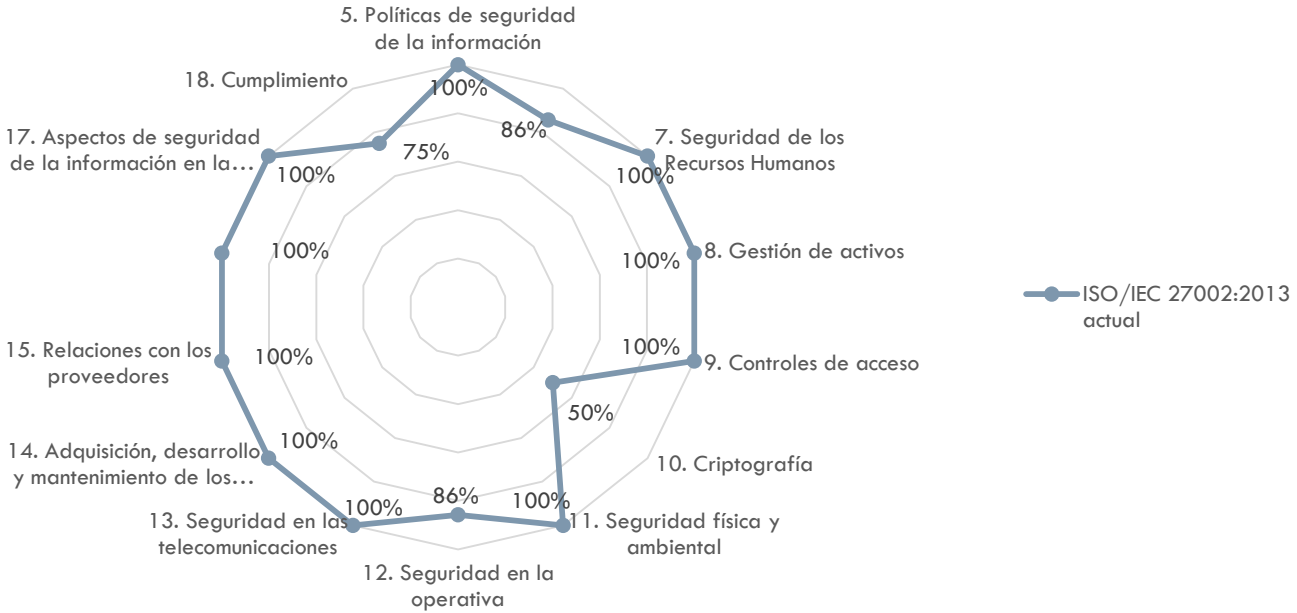
Inicial: 3. Establecido
Previsto: 3. Establecido
Actual: L3. Procedo definido

# 5. Auditoría de Cumplimiento: Presentación de Resultados

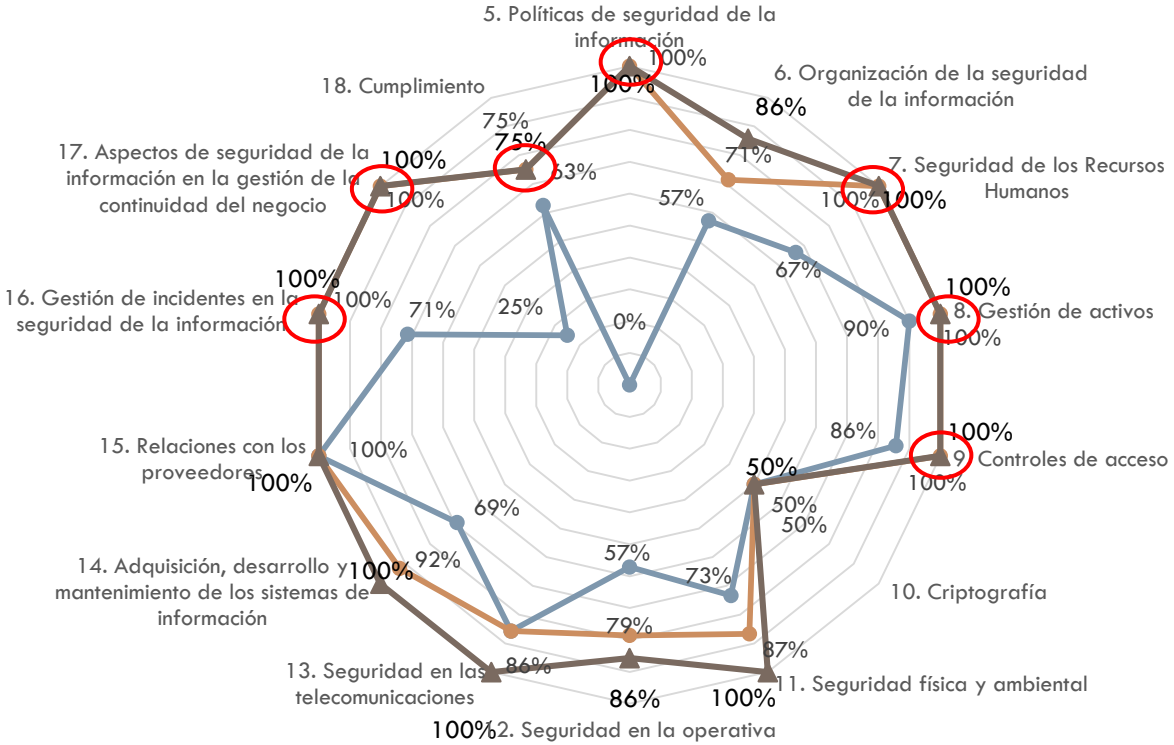


# 5. Auditoría de Cumplimiento: Presentación de Resultados

## Estado de madurez CMM ISO/IEC 27002:2013



# 5. Auditoría de Cumplimiento: Presentación de Resultados



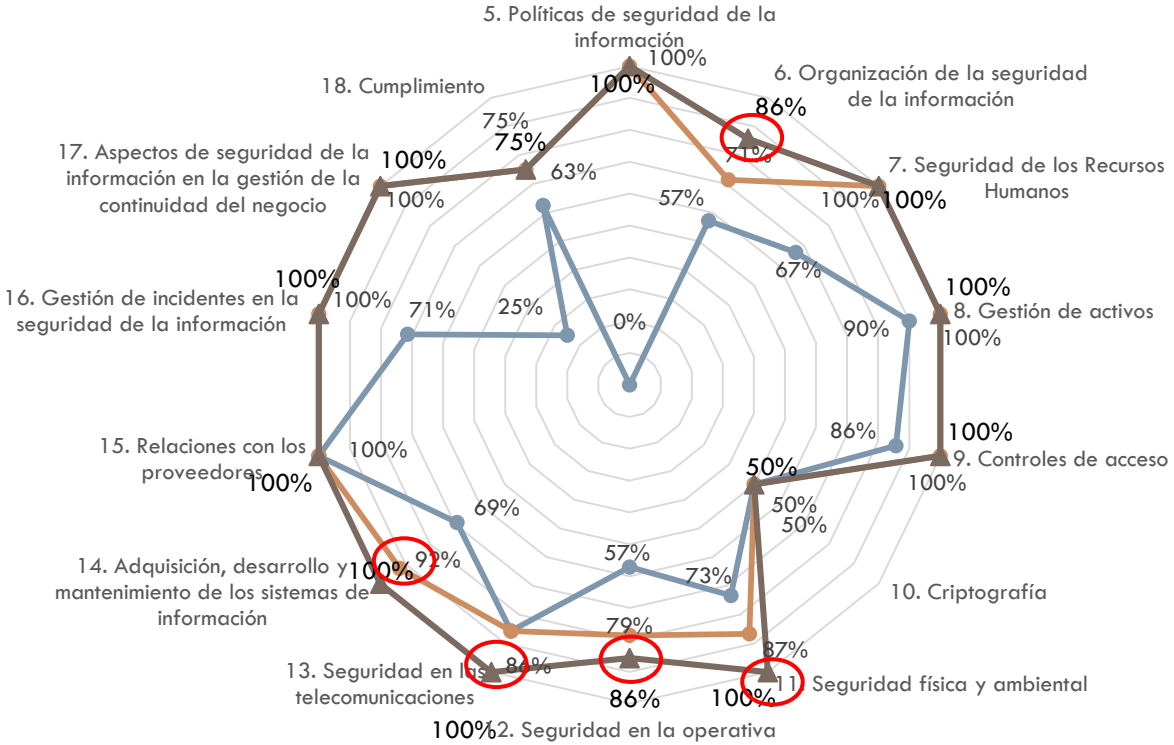

En 7 dominios el estado de madurez es igual al esperado

ISO/IEC 27002:2013 inicial

ISO/IEC 27002:2013 previsto

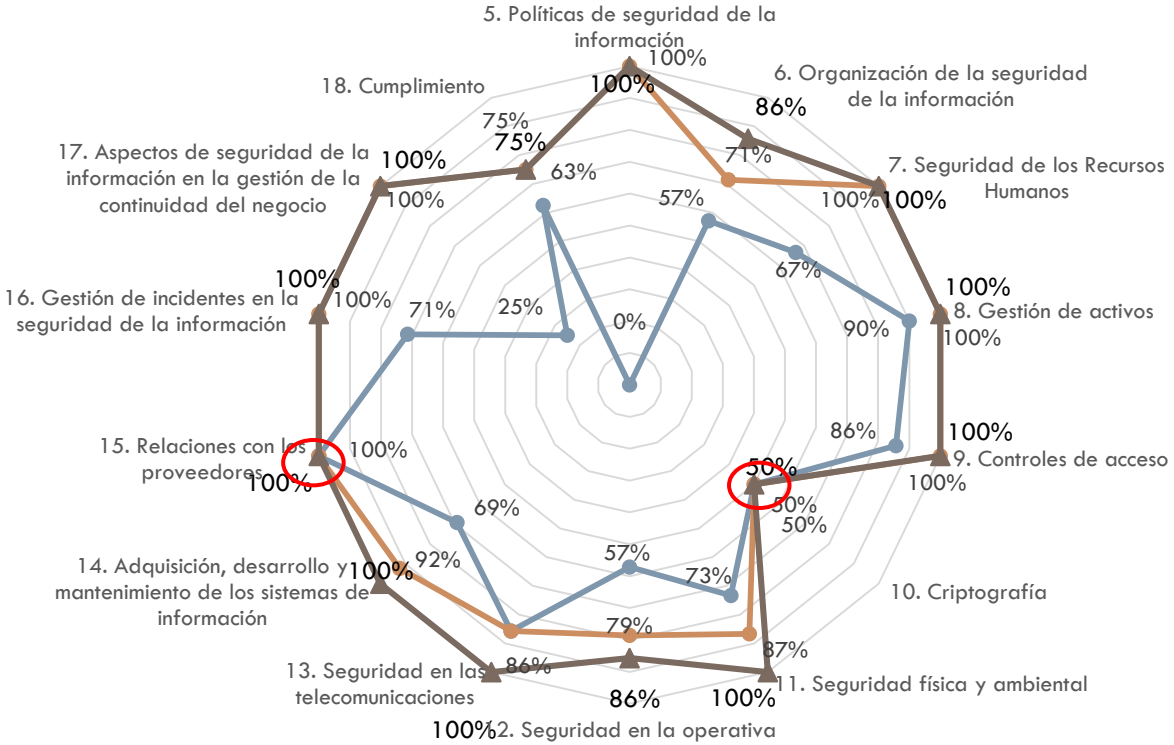
ISO/IEC 27002:2013 actual

# 5. Auditoría de Cumplimiento: Presentación de Resultados




En 5 dominios el estado de madurez supera lo esperado

# 5. Auditoría de Cumplimiento: Presentación de Resultados




En 2 dominios el estado de madurez no ha cambiado del estado inicial

# 5. Auditoría de Cumplimiento: Conclusiones

- El 28% de controles se encuentran con un proceso definido y ejecutado en donde la IES participa en el proceso, por lo tanto las capacitaciones planteadas han dado buenos resultados.
- El 20% se encuentra en un estado inicial /ad-hoc y reproducible pero intuitivo, esto se debe a que el mismo personal está generando políticas, lo cual es positivo, ya que tratan de generar sus procedimientos, que obviamente posterior deberán ser elevados al Consejo Superior para su aprobación.
- El 16% de procesos se encuentran en un estado optimizado, es decir, se encuentran bajo constante mejora.

# 5. Auditoría de Cumplimiento: Conclusiones

- El 5% no posee una política establecida, estas son las conformidades mayores presentadas en el apartado anterior.
- Cabe señalar, que se observó que ningún proceso tuvo una caída, es decir, el control presentaba el mismo estado o superior a lo que tenía en el estado actual al momento de inicializar el plan de implementación de la norma ISO/IEC 27001: 2013.

# Anexos

- Anexo 01 AnalisisDiferencial_27K (SGSI_OT_AD_2015-01)
- Anexo 02 Manual de Documentación (SGSI_MA_DO_2015-01)
- Anexo 03 Política de Seguridad (SGSI_PO_SI_2015-01)
- Anexo 04 Procedimiento de Auditorías Internas (SGSI_PR_AI_2015-01)
- Anexo 05 Gestión de Indicadores (SGSI_PR_I_2015-01)
- Anexo 06 Procedimiento de Revisión por la Dirección (SGSI_PR_RD_2015-01)
- Anexo 07 Gestión de Roles y Responsabilidades (SGSI_PR_RR_2015-01)
- Anexo 08 Metodología de Análisis de Riesgos (SGSI_PR_AR_2015-01)
- Anexo 09 Declaración de Aplicabilidad (SGSI_OT_DA_2015-01)
- Anexo 10 Análisis de Riesgos (SGSI_OT_AR_2015-01)
- Anexo 11 Plan de Gestión de Riesgos (SGSI_OT_GR_2015-01)
- Anexo 12 Auditoría de Cumplimiento (SGSI_OT_AC_2015-01