SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

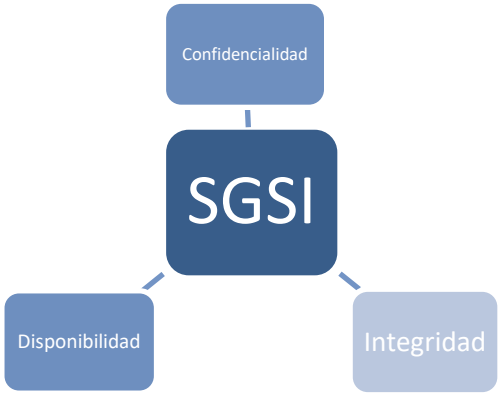
Estudiante: Luis Fernando Echeverría
Programa: Máster Interuniversitario en Seguridad de las TIC (MISTIC)
Consultor: Antonio José Segovia Henares.
Centro: Universitat Oberta de Catalunya.
Entrega: Enero de 2018.

CONTENIDO

- OBJETIVO DEL PROYECTO
- JUSTIFICACION
- DESARROLLO DEL PROYECTO
- CONCLUSIONES

OBJETIVO DEL PROYECTO

Analizar a profundidad los Sistemas de la Información de una determinada institución, en base a normativas y estándares internacionales (como ISO 27001 e ISO27002) para proponer acciones a modo de proyectos que contribuyan a mejorar la seguridad en base a un sistema de gestión.



NORMA DE REFERENCIA ISO/IEC 27001:2013

- Específica los requisitos para establecer, implementar, mantener y mejorar de manera continúa el SGSI dentro del contexto de una organización.
- Los requisitos son genéricos y son aplicables a todo tipo de organizaciones, independientemente tamaño naturaleza.
- Es una norma certificable.

JUSTIFICACION

Proteger los principales activos de la institución que son:

- la información y
- los sistemas de procesamiento de información.

Es importante para la institución garantizar una gestión adecuada de la seguridad de la información.

DESARROLLO DEL PROYECTO

FASE 1.- Situación Actual

FASE 2.- Sistema de Gestión Documental

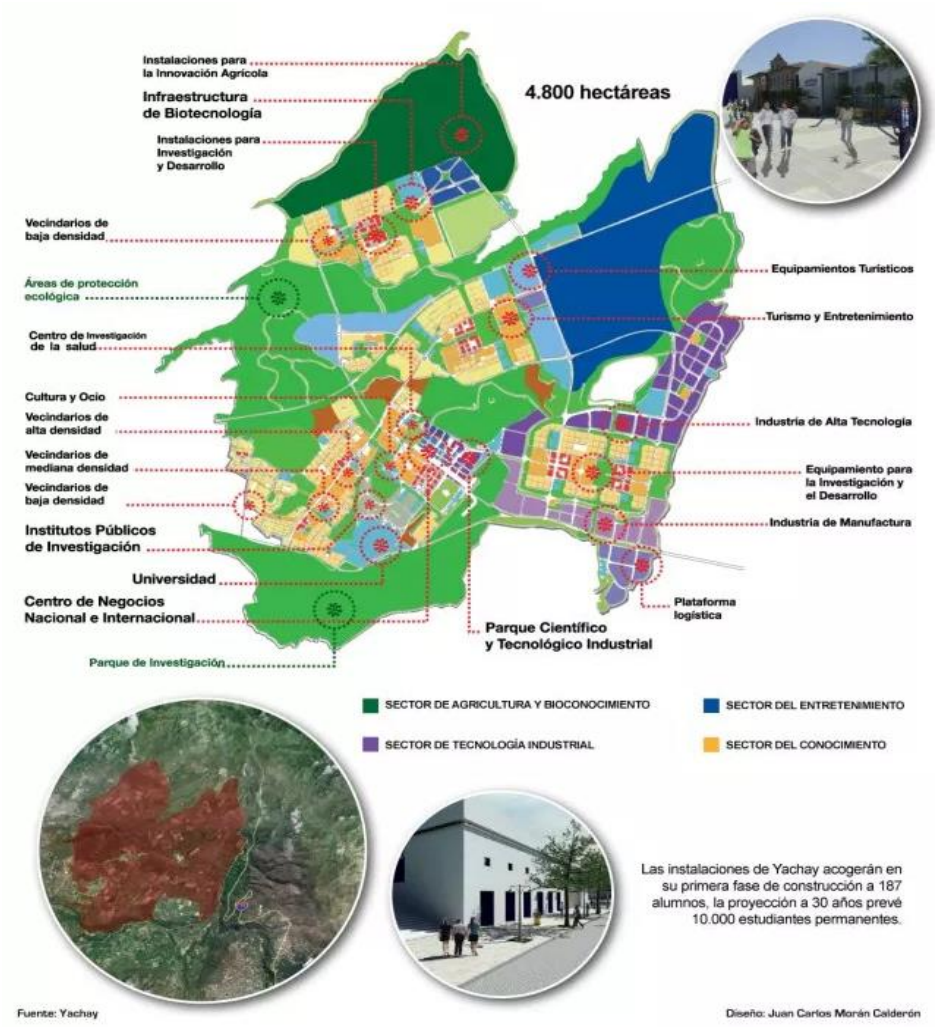
FASE 3.- Análisis de Riesgos

FASE 4.- Propuestas de Proyectos

FASE 5.- Auditoria de Cumplimiento

FASE 6.- Presentación de Resultados y Entrega de Informes

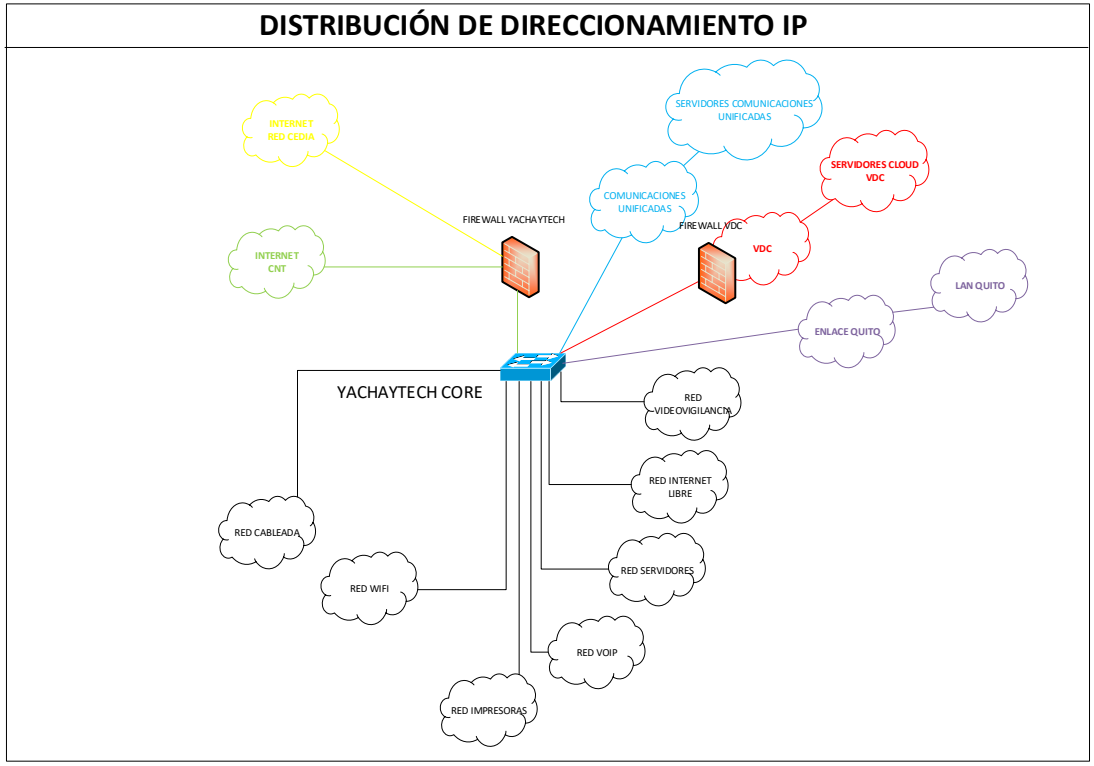
FASE 1: SITUACION ACTUAL



Contexto …

Arquitectura de TICs

Actualmente la institución cuenta con dos centros de procesamiento un local y un IaaS, tiene 32 servicios de TI, a continuación se presenta el diagrama de red:

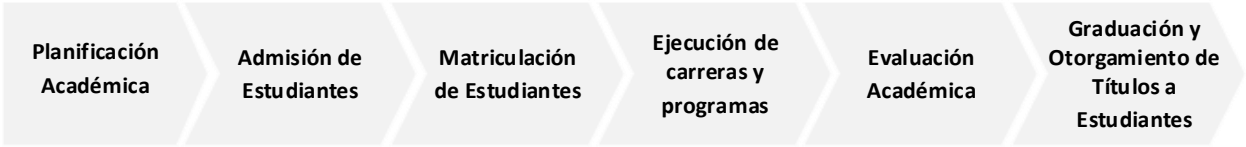


Objetivos especificos del Plan

- Crear proyectos basados en los resultados obtenidos en el análisis de riesgos y que estén alineados de acuerdo a las normas ISO/IEC 27001 e ISO/IEC 27002.
- Definir directrices en materia de la seguridad de la información.
- Identificar el nivel de seguridad existente en los sistemas, servicios y aplicaciones en la administración de la información.
- Identificar los riesgos a los cuales están expuestos los activos de la institución.
- Definir los roles, las responsabilidades en materia de seguridad para estudiantes, docentes y personal administrativo.
- Crear y promover la cultura de seguridad de la información dentro de la institución.
- Implantar y hacer un seguimiento del plan de seguridad definido.

Alcance

Se define para el alcance de la implementación del SGSI, los procesos medulares que se encuentran dentro de los Procesos Agregado de Valor de docencia, los mismos que son:



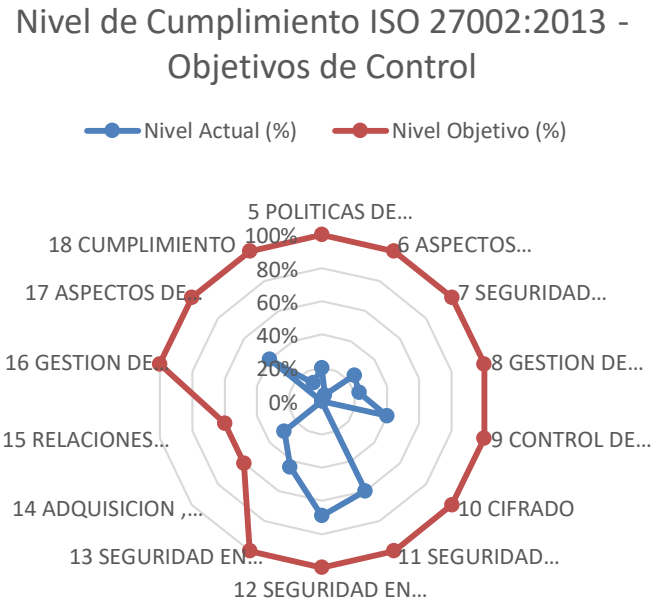
Procesos Agregado de Valor para el SGSI.

Cabe mencionar que el proceso de Graduación y Otorgamiento de Títulos a Estudiantes no se considera debido a que la institución comenzó a funcionar en el abril de 2014 por lo que se tendrá a los primeros graduados en el año 2019.
Dentro de los procesos participan las siguientes áreas:

- Coordinación Administrativa Financiera,
- Coordinación de Tecnologías de la Información,
- Coordinación de Servicios Escolares,
- Coordinación de Intercambio Académico,
- Coordinación de Bienestar Estudiantil,
- Vicecancillería de Asuntos Académico, y
- Decanatos.

Estado actual de la seguridad

CONTROL	Nivel de Cumplimiento (%)
5 POLITICAS DE SEGURIDAD	20%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	4%
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	25%
8 GESTION DE ACTIVOS	23%
9 CONTROL DE ACCESO	40%
10 CIFRADO	0%
11 SEGURIDAD FISICA Y AMBIENTAL	60%
12 SEGURIDAD EN LA OPERATIVA	55%
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	44%
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	29%
15 RELACIONES CON SUMINISTRADORES.	40%
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	0%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40%
18 CUMPLIMIENTO	12%



FASE 2: SISTEMA DE GESTION DOCUMENTAL

- Política de Seguridad
- Procedimiento de Auditorias Internas
- Gestión de Indicadores
- Procedimiento Revisión por la Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis de Riesgo
- Declaración de Aplicabilidad

FASE 3: ANALISIS DE RIESGOS

- Inventario de activos
- Valoración de activos
- Dimensiones de seguridad
- Tabla resumen de valoración
- Análisis de amenazas
- Impacto potencial
- Nivel de Riesgo Aceptable y Residual

INVENTARIO DE ACTIVOS

Se han agrupado los activos en grupos acordes a la metodología MAGERIT:

- Instalaciones
- Hardware
- Software
- Datos
- Red
- Servicios
- Equipamiento auxiliar
- Personal

VALORACIÓN DE ACTIVOS

Valoración	Rango	Valor
Muy alta	valor > 200.000 USD	300.000 USD
Alta	100.000 USD< valor > 200.000 USD	150.000 USD
Media	50.000 USD< valor > 100.000 USD	75.000 USD
Baja	10.000 USD< valor > 50.000 USD	30.000 USD
Muy baja	valor < 10.000 USD	10.000 USD

Tabla de valoración de activos.

DIMENSIÓN DE SEGURIDAD

Una vez se tenga el valor del activo se debe considerar el nivel de protección que se requiere en la(s) dimensión(es) de seguridad estas pueden ser:

- Autenticidad (**A**): garantías de identidad de los usuarios.
- Confidencialidad (**C**): accesos a información sensible.
- Integridad (**I**): garantía de que los métodos de acceso a la información son completos.
- Disponibilidad (**D**): garantía de disponibilidad máxima de la información.
- Trazabilidad (**T**): garantía de revisión de acciones sobre la información.

Las mismas que se deben valorar por nivel de daño, escala de valoración es:

Valoración	Criterio
10	Daño Muy grave
7-9	Daño Grave
4-6	Daño Importante o considerable
1-3	Daño Menor
0	Irrelevante

Tabla de valoración para las dimensiones de seguridad.

TABLA RESUMEN DE VALORACIÓN

Ámbito	Activo	Valor	Aspectos críticos				
			A	C	I	D	T
Instalaciones	Data Center - El Rosario	MUY ALTA	8	8	8	10	10
Instalaciones	Cuarto de Rack - San José	MEDIA	8	8	8	10	10
Instalaciones	Cuarto de Rack - Ingenio - Principal	ALTA	8	8	8	10	10
Instalaciones	Cuarto de Rack - Ingenio - Biblioteca	ALTA	8	8	8	10	10
Instalaciones	Cuarto de Rack - Ingenio – Aulas	ALTA	8	8	8	10	10
Red	Puntos de Red – Cableado Estructurado – Servidores - El Rosario	MEDIA	8	6	8	10	8
Red	Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	MEDIA	8	6	8	10	8
Red	Puntos de Red – Cableado Estructurado – Puestos de Trabajo – Ingenio	MEDIA	8	6	8	10	8
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	BAJA	8	6	6	10	8
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	BAJA	8	6	6	10	8
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red – Ingenio	BAJA	8	6	6	10	8
Red	Switch Core - El Rosario	MUY ALTA	9	8	6	10	8
Red	Switch 24 puertos - El Rosario	MEDIA	9	8	6	8	8
Red	Switch 24 puertos – Ingenio	MEDIA	8	8	8	8	8
Red	Switch 48 puertos - El Rosario – Residencias	MEDIA	8	8	8	8	8

Tabla de valoración de activos

ANALISIS DE AMENAZAS

Para la identificación de las amenazas se utiliza la tabla establecida en MAGERIT, se tiene tres tipos de amenazas que son de origen: Natural, Industrial, y Humano (Intencional y No Intencional) (Anexo 10).

ID	ORIGEN	AMENAZAS
[N.1]	Desastres naturales	Fuego
[N.2]	Desastres naturales	Daños por agua
[N.*]	Desastres naturales	Desastres naturales
[I.1]	De origen industrial	Fuego
[I.2]	De origen industrial	Daños por agua
[I.*]	De origen industrial	Desastres industriales
[I.3]	De origen industrial	Contaminación mecánica
[I.4]	De origen industrial	Contaminación electromagnética
[I.5]	De origen industrial	Avería de origen físico o lógico
[I.6]	De origen industrial	Corte del suministro eléctrico
[I.7]	De origen industrial	Condiciones inadecuadas de temperatura o humedad
[I.8]	De origen industrial	Fallo de servicios de comunicaciones
[I.9]	De origen industrial	Interrupción de otros servicios y suministros esenciales
[I.10]	De origen industrial	Degradación de los soportes de almacenamiento de la información
[I.11]	De origen industrial	Emanaciones electromagnéticas
[E.1]	Errores y fallos no intencionados	Errores de los usuarios
[E.2]	Errores y fallos no intencionados	Errores del administrador
[E.3]	Errores y fallos no intencionados	Errores de monitorización (log)
[E.4]	Errores y fallos no intencionados	Errores de configuración

ANALISIS DE AMENAZAS

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- degradación: cuán perjudicado resultaría el activo
- probabilidad (frecuencia): cuán probable o improbable es que se materialice la amenaza

Por cada amenaza detectada se debe establecer la frecuencia que el activo es presumido, se clasifica la frecuencia, se toma como máximo el valor 1, que quiere decir que la amenaza está presente el 100% de días del año (365 días). Partiendo de esto, se crea la siguiente escala:

FRECUENCIA		
VALORACIÓN	RANGO (EN ITERACIONES)	ID
Muy alta	1 (cada día)	PR-MA
Alta	0,0712 (cada 2 semanas)	PR-A
Media	0,0164 (cada 2 meses)	PR-M
Baja	0,0054 (cada semestre)	PR-B
Muy Baja	0,0027 (cada año)	PR-MB

Tabla de Frecuencia

ANALISIS DE AMENAZAS

Tabla de degradación dimensiones de la seguridad por amenaza y frecuencia

Ámbito	Activo	Amenaza	Frecuencia	Degradación				
				A	C	I	D	T
Instalaciones	Data Center - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Instalaciones	Data Center - El Rosario	[I.*]	PR-MB	0%	0%	0%	100%	0%
Instalaciones	Data Center - El Rosario	[I.6]	PR-B	0%	0%	0%	100%	0%
Instalaciones	Data Center - El Rosario	[A.11]	PR-MB	0%	40%	0%	100%	100%
Instalaciones	Cuarto de Rack - San José	[N.*]	PR-MB	0%	0%	0%	100%	0%
Instalaciones	Cuarto de Rack - San José	[I.*]	PR-MB	0%	0%	0%	100%	0%
Instalaciones	Cuarto de Rack - San José	[I.6]	PR-B	0%	0%	0%	100%	0%
Instalaciones	Cuarto de Rack - Ingenio - Principal	[N.*]	PR-MB	0%	0%	0%	100%	0%
Instalaciones	Cuarto de Rack - Ingenio - Principal	[I.*]	PR-MB	0%	0%	0%	100%	0%
Instalaciones	Cuarto de Rack - Ingenio - Principal	[I.6]	PR-B	0%	0%	0%	100%	0%
Instalaciones	Cuarto de Rack - Ingenio - Biblioteca	[N.*]	PR-MB	0%	0%	0%	100%	0%
Instalaciones	Cuarto de Rack - Ingenio - Biblioteca	[I.*]	PR-MB	0%	0%	0%	100%	0%
Red	Switch 24 puertos - Ingenio	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Switch 24 puertos - Ingenio	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Switch 24 puertos - Ingenio	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Switch 24 puertos - Ingenio	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Switch 48 puertos - El Rosario - Residencias	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Switch 48 puertos - El Rosario - Residencias	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Switch 48 puertos - El Rosario - Residencias	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Switch 48 puertos - El Rosario - Residencias	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Switch 48 puertos - El Rosario - Residencias	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Routers Inalambricos - Ingenio	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Firewall - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Firewall - El Rosario	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Firewall - El Rosario	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Firewall - El Rosario	[A.11]	PR-MB	60%	40%	40%	100%	80%
Red	Firewall - El Rosario	[A.24]	PR-MB	0%	0%	0%	100%	0%
Red	Routers - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Routers - El Rosario	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Routers - El Rosario	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Routers - El Rosario	[E.28]	PR-B	0%	0%	0%	100%	0%

IMPACTO POTENCIAL

Para esto se procede a calcular el Impacto aplicando la metodología (Ver ANEXO X) en donde se realiza un cruce entre el valor de activo con la degradación en las diferentes dimensiones de seguridad que se ve afectado por una amenaza.

IMPACTO		Degradación				
		1 - 4 %	5 - 24%	25 - 49 %	50 - 74%	75 -100%
Valor activo	MA	M	A	MA	MA	MA
	A	B	M	A	MA	MA
	M	MB	B	M	A	A
	B	MB	MB	B	M	M
	MB	MB	MB	MB	B	B

RIESGO POTENCIAL

Para este paso se valora el nivel de riesgo para el SGSI. Se determinará el riesgo que probabilidad que tenga una amenaza.

Para este caso se estable un cuadro de nivel de riesgo, ver tabla:

Riesgo		Probabilidad (Frecuencia)				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

Impacto Residual.- Dado un cierto conjunto de salvaguardas (contramedidas) desplegadas y una medida de la madurez del proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual, se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

Riesgo Residual.- Dado un cierto conjunto de salvaguardas (contramedidas) desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual, se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

Es necesario definir un límite a partir del cual podamos decidir si asumir un riesgo o por el contrario no asumirlo y por tanto aplicar controles. Para la actual propuesta se establece que el nivel de riesgo aceptable es “Alto”, todo lo que esté por debajo de este nivel de riesgo, no supondrá una amenaza importante para la institución, y por tanto no es de interés. Por lo tanto, el nivel de riesgo que supera el aceptable, se tendrá que establecer controles para reducirlo.

Tabla de Riesgo Residual

Activo	Amenaza	Frecuencia	RIESGO				
			A	C	I	D	T
Data Center - El Rosario	[N.*]	PR-MB				A	
Data Center - El Rosario	[I.*]	PR-MB				A	
Data Center - El Rosario	[I.6]	PR-B				MA	
Data Center - El Rosario	[A.11]	PR-MB		A		A	A
Cuarto de Rack - San José	[N.*]	PR-MB				M	
Cuarto de Rack - San José	[I.*]	PR-MB				M	
Cuarto de Rack - San José	[I.6]	PR-B				A	
Cuarto de Rack - Ingenio - Principal	[N.*]	PR-MB				A	
Cuarto de Rack - Ingenio - Principal	[I.*]	PR-MB				A	
Cuarto de Rack - Ingenio - Principal	[I.6]	PR-B				MA	
Cuarto de Rack - Ingenio - Biblioteca	[N.*]	PR-MB				A	
Cuarto de Rack - Ingenio - Biblioteca	[I.*]	PR-MB				A	
Cuarto de Rack - Ingenio - Biblioteca	[I.6]	PR-B				MA	
Cuarto de Rack - Ingenio - Aulas	[N.*]	PR-MB				A	
Cuarto de Rack - Ingenio - Aulas	[I.*]	PR-MB				A	
Cuarto de Rack - Ingenio - Aulas	[I.6]	PR-B				MA	
Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[N.*]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[E.25]	PR-MB				M	

IMPACTO DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

Los principales activos afectados si se materializa la amenaza son:

Ambito	Activo
Instalaciones	Data Center - El Rosario
Red	Switch Core - El Rosario
Red	Firewall - El Rosario
Software	Motor de Base de Datos - Servicios de Gestión Académica.
Software	Servidor Directorio Activo - Toda la Institución
Software	Servidor de Backup Archivos - Servicios de Gestión Académica.
Datos	Base de Datos Estudiantes - Servicios de Gestión Académica.
Datos	Base de Datos Docentes - Servicios de Gestión Académica.
Datos	Base de Datos Personal Administrativo - Toda la Institución
Servicios	IaaS – CNT
Servicios	Sistema Académico - Power Campus
Servicios	Sistema Virtual de Aprendizaje - D2L
Servicios	Usuario Externo -

Principales activos amenazados

La consecuencia donde se vería afectado a las dimensiones de seguridad son: Disponibilidad en un 100%; en Autenticación, Confidencialidad y Trazabilidad en un 80% y en Integridad en un 75%.

FASE 4: PROPUESTAS DE PROYECTOS

PROYECTOS	PLAZO
PRJ-01 Implantación de políticas de seguridad de la información.	CORTO PLAZO
PRJ-02 Instalación de un sistema de respaldos y recuperación.	
PRJ-03 Migración de dispositivos de seguridad de red (firewall/IDS/IPS).	
PRJ-04 Repotenciar Data Center.	
PRJ-05 Plan de formación y concientización	
PRJ-06 Políticas de control de acceso a la red y servicios de red	
PRJ-07 Gestión del acceso del usuario	MEDIANO PLAZO
PRJ-08 Control de acceso al sistema y aplicaciones	
PRJ-09 Mejora en la gestión de Recursos Humanos	LARGO PLAZO
PRJ-10 Clasificación de la Información	
PRJ-11 Implementar un CSIRT	

FASE 4: PROPUESTAS DE PROYECTOS

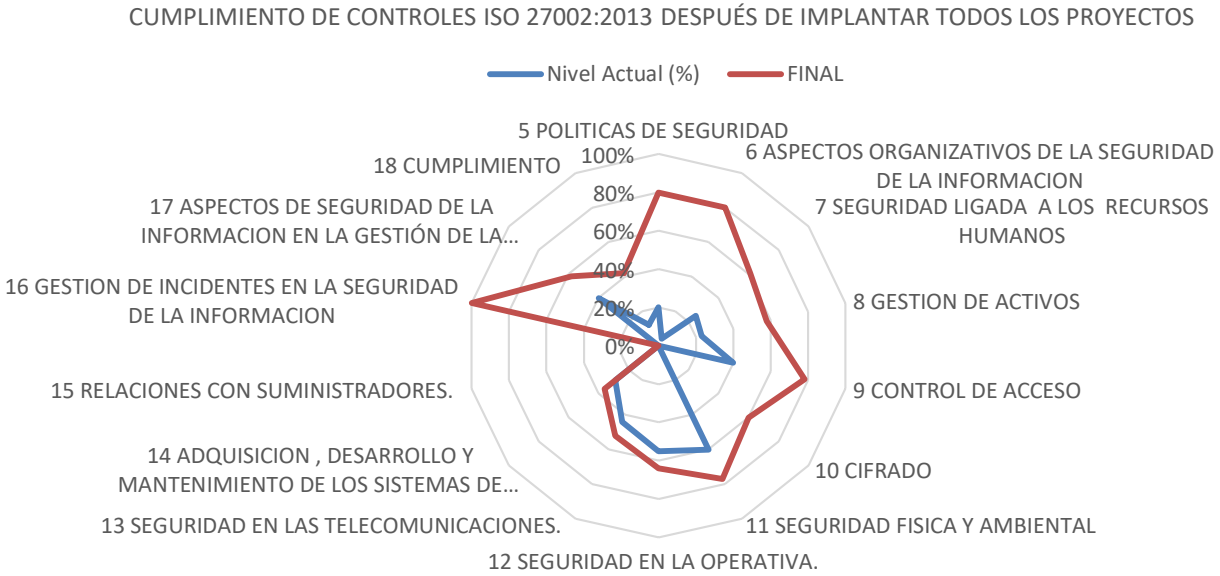
PLAN DE IMPLEMENTACIÓN	PERIODO											
PROYECTOS	1 TRIMESTRE	2 TRIMESTRE	3 TRIMESTRE	4 TRIMESTRE	1 TRIMESTRE	2 TRIMESTRE	3 TRIMESTRE	4 TRIMESTRE	1 TRIMESTRE	2 TRIMESTRE	3 TRIMESTRE	4 TRIMESTRE
PRJ-01 Implantación de políticas de seguridad de la información.												
PRJ-02 Instalación de un sistema de respaldos y recuperación.												
PRJ-03 Migración de dispositivos de seguridad de red (firewall/IDS/IPS).												
PRJ-04 Repotenciar Data Center.												
PRJ-05 Plan de formación y concientización												
PRJ-06 Políticas de control de acceso a la red y servicios de red												
PRJ-07 Gestión del acceso del usuario												
PRJ-08 Control de acceso al sistema y aplicaciones												
PRJ-09 Mejora en la gestión de Recursos Humanos												
PRJ-10 Clasificación de la Información												
PRJ-11 Implementar un CSIRT												

CUMPLIMIENTO DESPUES DE LA IMPLEMENTACION DE PROYECTOS

CONTROL	Nivel Actual (%)	FINAL
5 POLITICAS DE SEGURIDAD	20%	80%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	4%	80%
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	25%	61%
8 GESTION DE ACTIVOS	23%	58%
9 CONTROL DE ACCESO	40%	78%
10 CIFRADO	0%	60%
11 SEGURIDAD FISICA Y AMBIENTAL	60%	77%
12 SEGURIDAD EN LA OPERATIVA.	55%	64%
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	44%	52%
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	29%	36%
15 RELACIONES CON SUMINISTRADORES.	40%	40%
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	0%	100%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40%	58%
18 CUMPLIMIENTO	12%	42%
PORCENTAJE DE MADUREZ	**27%**	**65%**

EVOLUCION DE LOS DOMINIOS

De acuerdo al modelo CMM el nivel general de cumplimiento de los diferentes controles antes de la implementación, es “Inicial/AD-HOC”. El nivel de cumplimiento general después de la implementación de los proyectos propuestos sube al nivel de “Reproducible, pero intuitivo” y para ciertos dominios siguen en un estado “Inicial/AD-HOC”. El porcentaje de cumplimiento después de la implementación de los proyectos sube de 27% a 65%.



FASE 5: AUDITORIA DE CUMPLIMIENTO

Se evalúa el nivel de cumplimiento con las buenas prácticas en materia de seguridad.

Marco de referencia ISO/IEC 27002:2013

Antes de continuar con la metodología, se debe considerar los diferentes aspectos en los cuales las salvaguardas actúan reduciendo el riesgo, ya hablemos de los controles ISO/IEC 27002:2013 o de cualquier otro catálogo.

Estos son en general:

- Formalización de las prácticas mediante documentos escritos o aprobados.
- Política de personal.
- Solicitudes técnicas (software, hardware o comunicaciones).
- Seguridad física.

La protección integral frente a las posibles amenazas, requiere de una combinación de salvaguardas sobre cada uno de estos aspectos.

FASES

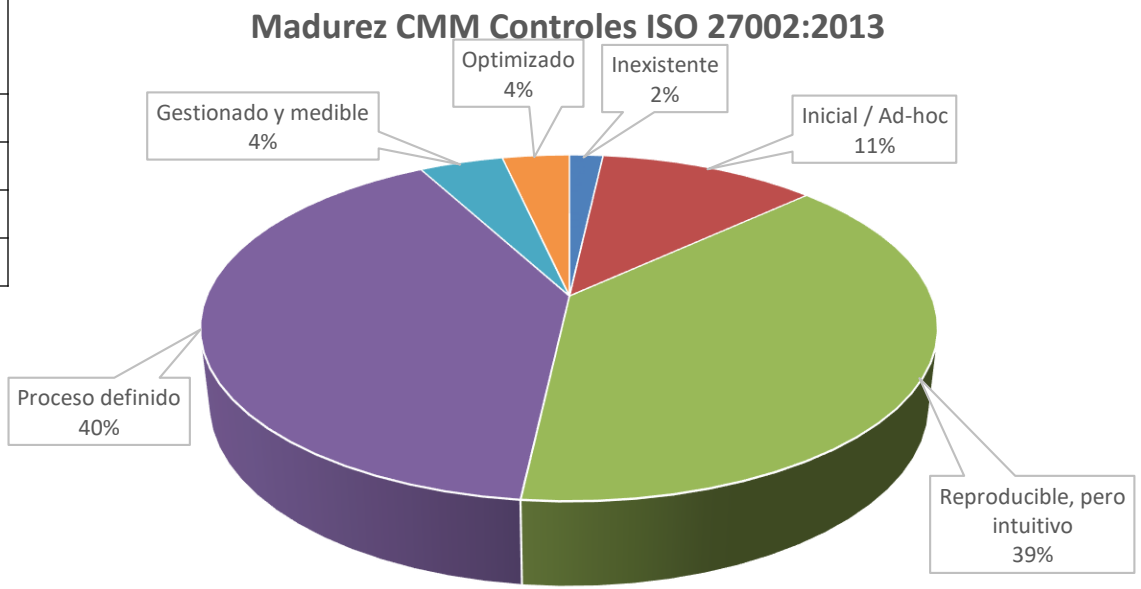
- Fase 1: Recolección de la información
- Fase 2: Ejecución de pruebas documentadas
- Fase 3: Análisis de la información
- Fase 4: Elaboración y presentación del Reporte de la Auditoria

FASE 5: AUDITORIA DE CUMPLIMIENTO

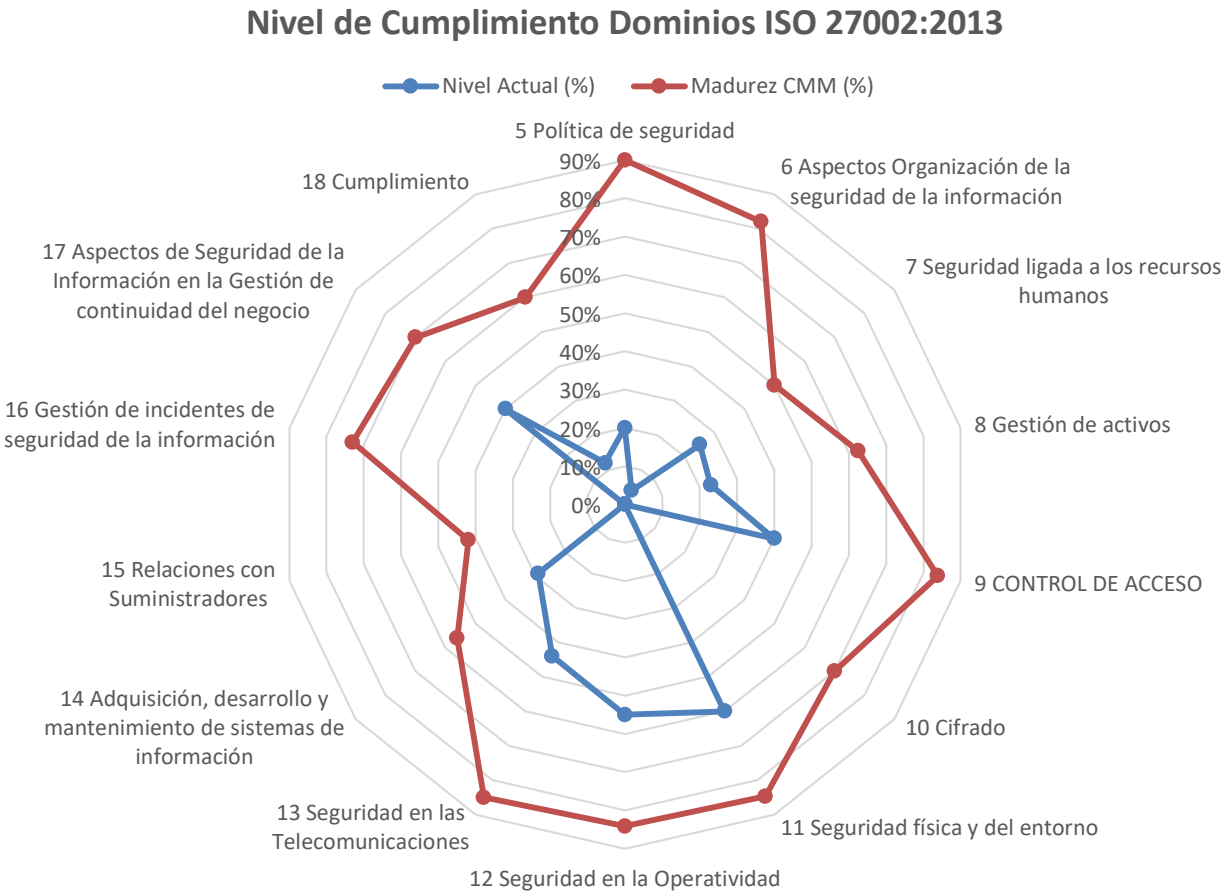
EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces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

FASE 5: AUDITORIA DE CUMPLIMIENTO

Nivel de Madurez	Cuenta de Controles ISO 27002:2013
Inexistente	2
Inicial / Ad-hoc	13
Reproducible, pero intuitivo	44
Proceso definido	46
Gestionado y medible	5
Optimizado	4
Total general	114

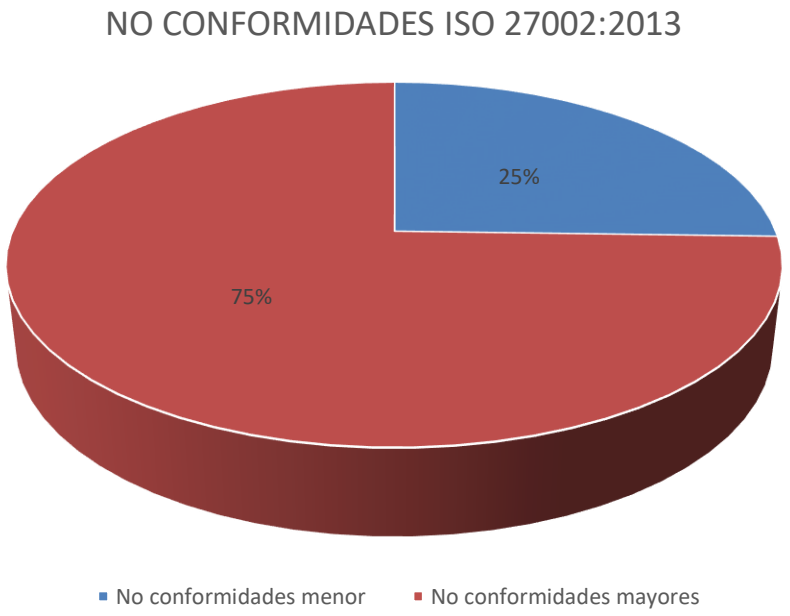


FASE 5: AUDITORIA DE CUMPLIMIENTO



FASE 5: AUDITORIA DE CUMPLIMIENTO

DOMINIOS	NO CONFORMIDADES	
	MAYORES	MENORES
5 POLITICAS DE SEGURIDAD	1	
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	1	
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		6
8 GESTION DE ACTIVOS		7
9 CONTROL DE ACCESO		3
10 CIFRADO		1
11 SEGURIDAD FISICA Y AMBIENTAL		3
12 SEGURIDAD EN LA OPERATIVA.	2	2
13 SEGURIDAD EN LAS TELECOMUNICACIONES.		1
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION		10
15 RELACIONES CON SUMINISTRADORES.	3	
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION		
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	7	2
18 CUMPLIMIENTO		6
TOTAL	14	41



FASE 6 : PRESENTACION DE RESULTADOS

- Memoria
- Informe Ejecutivo
- Presentacion (video)

CONCLUSIONES DEL PROYECTO

- La institución a ser relativamente nueva tiene la oportunidad de introducir las normas con mayor facilidad por lo que se puede ampliar el alcance del proyecto a los demás procesos que vayan surgiendo de la entidad.
- La implementación de un Plan de Seguridad de la Información es un proceso continuo que busca mejorar de los niveles de Seguridad en el manejo de la Información y que esté acorde a las necesidades institucionales.
- De acuerdo a los resultados este plan ha mejorado el nivel de seguridad de la información en la institución.

CONCLUSIONES DEL PROYECTO

- Requiere de la participación y el compromiso de todos los miembros de la institución (estudiantes, docentes y personal administrativo) y principalmente de la Dirección.
- Se ha creado una estructura interna con roles y responsabilidades directa sobre la seguridad de la información.
- Este plan debe ser la única guía corporativa que implementa las medidas de seguridad de la información y los sistemas de información dentro de la institución.
- El proceso de formación/concientización es fundamental para la evolución exitosa de este plan. Si bien se ha logrado mejorar los niveles de concientización del personal, se recomienda que el proceso de formación sea continua.