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: Febrero de 2018.

Índice

1 Situación actual: Contextualización, Objetivos y Análisis Diferencial

1.1 Introducción

En cualquier organización, sea pública o privada; pequeña o grande, es necesario conocer el estado de los Sistemas y Tecnologías de la Información para determinar si son adecuados y seguros para desarrollar las actividades de forma satisfactoria. En la última década los ataques e incidentes de seguridad de la información no sólo han ocurrido en instituciones relacionadas con los sectores de seguridad nacional, financieros, productivos o de infraestructuras críticas, sino también en entidades académicas dedicadas a desarrollar proceso de investigación y docencia, información que lo reporta el informe de la OEA (OEA y Symantec, 2014); en el cual, señalan que las entidades del ámbito académico son afectadas en un 39% por delitos informáticos.

Particularmente, se presenta esta situación en aquellas instituciones educativas que cuentan con programas avanzados de investigación, ya que manejan información de carácter reservado o confidencial; desarrollan conocimiento científico y tecnología con el respaldo y financiamiento de organizaciones para resolver problemas o necesidades complejas de la sociedad; en aquellas que manejan datos personales de su comunidad (alumnos, profesores, investigadores y directivos); datos de su programa académico; entre otros; y finalmente ocupan activos de TI para su almacenamiento y procesamiento.

Considerando los aspectos señalados anteriormente y los incidentes de seguridad que se han presentado en la institución; se plantea el presente proyecto denominado Sistema de Gestión de la Seguridad de la Información que corresponde al Trabajo Final del Master Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones despliega la metodología y actividades requeridas para la elaboración de un Plan Director de Seguridad, orientado a la implementación de la norma ISO/EIC 27001:2013 – Sistema de Gestión de la Seguridad de la Información y que contribuirá a mitigar riesgos contra la seguridad de la información que es parte de los objetivos de la entidad.

1.2 Conociendo la ISO/IEC 27001

A medida que la seguridad se ha consolidado como una parte cada vez más importante de los sistemas de información, también lo ha ido haciendo la metodología y las ‘buenas prácticas’ sobre seguridad de la información. Por ello, se ha creído relevante disponer de una primera etapa donde

se documente algunas de las mejores prácticas en seguridad de la información para realizar una aproximación sistemática al análisis de la seguridad.

Aun cuando son muchas las aproximaciones, la propuesta se centrará en el estudio de la ISO/IEC 27001 y 27002, ya que estas especifican los requisitos para establecer, implementar, mantener y mejorar de manera continua el SGSI dentro del contexto de una organización. Es por ello, que, en esta fase, se documentara sobre la misma y se compartirán las impresiones o dudas que puedan generarse al respecto.

Para conocer un poco de las normas se comenzará a describir la evolución de la norma:

La ISO/IEC 27001 es la norma que establece los requisitos para implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, la ISO/IEC 27002 es la norma que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

Estos estándares internacionales fueron publicados como tal por la International Organization for Standardization y por la comisión International Electrotechnical Commission en octubre del año 2005 y actualmente, es el único estándar aceptado a nivel internacional para la gestión de la Seguridad de la Información.

A continuación, se hace un pequeño cuadro en donde cronológicamente se puede observar su evolución:

1901	Normas “BS”: La British Standards Institution publica normas con el prefijo “BS” con carácter internacional. Estas son el origen de normas actuales como ISO 9001, ISO 14001 u OHSAS 18001.
1995	BS 7799-1:1995: Mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Eran recomendaciones que no permitían la certificación ni establecía la forma de conseguirla.
1998	BS 7799-2:1999: Revisión de la anterior norma. Establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.
1999	BS 7799-1:1999: Se revisa.

2000	ISO/IEC 17799:2000: La Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799, sin experimentar grandes cambios.
2002	BS 7799-2:2002: Se publicó una nueva versión que permitió la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países.
2005	ISO/IEC 27001:2005 e ISO/IEC17799:2005: Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.
2007	ISO 17799: Se renombra y pasa a ser la ISO 27002:2005
2007	ISO/IEC 27001:2007: Se publica la nueva versión.
2009	Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M:2009.
2013	ISO/IEC 27001:2013: Este año 2013 se ha publicado ya la nueva versión de la ISO 27001 que trae cambios significativos en su estructura, evaluación y tratamiento de los riesgos. ISO/IEC 27002:2013: Este año 2013 se ha publicado ya la nueva versión de la ISO 27002 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 35 objetivos de control y 114 controles, agrupados en 14 dominios.

Adicionalmente, se complementará el presente proyecto con Magerit que es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas. Muy utilizada en España y parte de Iberoamérica; tiene la particularidad de expresar sus resultados en términos cuantitativos o cualitativos con lo que facilita la toma de decisiones. En el presente estudio se expresará los resultados en términos cualitativos porque “el modelo la captura de datos cualitativa es más ágil que la cuantitativa, los modelos cualitativos son eficaces relativizando lo más importante de lo que no es tan importante; pero agrupan las conclusiones en grandes grupos” (Amutio, Miguel,2012, p.124).

1.3 Objetivos del Trabajo

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.

1.4 Contextualización

La organización objeto de estudio y análisis, es una institución de educación superior pública orientada a la docencia e investigación; es considerada, uno de los proyectos emblemáticos y con gran visión para el estado Ecuatoriano. La institución tiene como fin orientar la formación científica, tecnológica e investigativa, para el desarrollo del país y América Latina.

Se encuentra ubicada en la ciudad de Urcuqui – Ecuador, fue creada el año 2013 y cuyo inicio académico comienza en abril de 2014, con 172 estudiantes, 20 docentes y aproximadamente 20 personas del área administrativa; actualmente cuenta con 761 estudiantes, 126 docentes y 165 administrativos.

Estructura Organizacional

De acuerdo al Estatuto Orgánico Funcional aprobado por el Consejo de Educación Superior (CES), se implanta la estructura organizacional y los procesos de la institución, que a continuación, se detalla:

Procesos

Las actividades que se desarrollan en la institución se constituyen en procesos necesarios para generar productos demandados por usuarios internos o externos. Se ordenan y clasifican en función de su grado de contribución o valor agregado al cumplimiento de la misión institucional:

a. **Procesos gobernantes. -** Son aquellos que orientan la gestión institucional a través de la formulación de políticas, la expedición de políticas, normas, procedimientos, planes, acuerdos, resoluciones y otros instrumentos o herramientas para el funcionamiento de la organización, la articulación, coordinación y establecimiento de mecanismos para la ejecución de los planes, programas, proyectos, directrices para el buen desempeño de la gestión institucional.

b. **Procesos agregadores de valor o misionales**. - Son los responsables de generar, administrar y controlar el portafolio de productos y servicios, destinados a usuarios

externos, permiten cumplir con la misión institucional, los objetivos estratégicos y constituyen la razón de ser de la Institución.

c. Procesos habilitantes (apoyo y asesoría). - Se clasifican en procesos de asesoría y procesos de apoyo, están encaminados a generar productos y servicios de asesoría y apoyo logístico para producir el portafolio de productos institucionales demandados por los procesos gobernantes, agregadores de valor y para sí mismos, viabilizando la gestión (Ver gráfico 1).

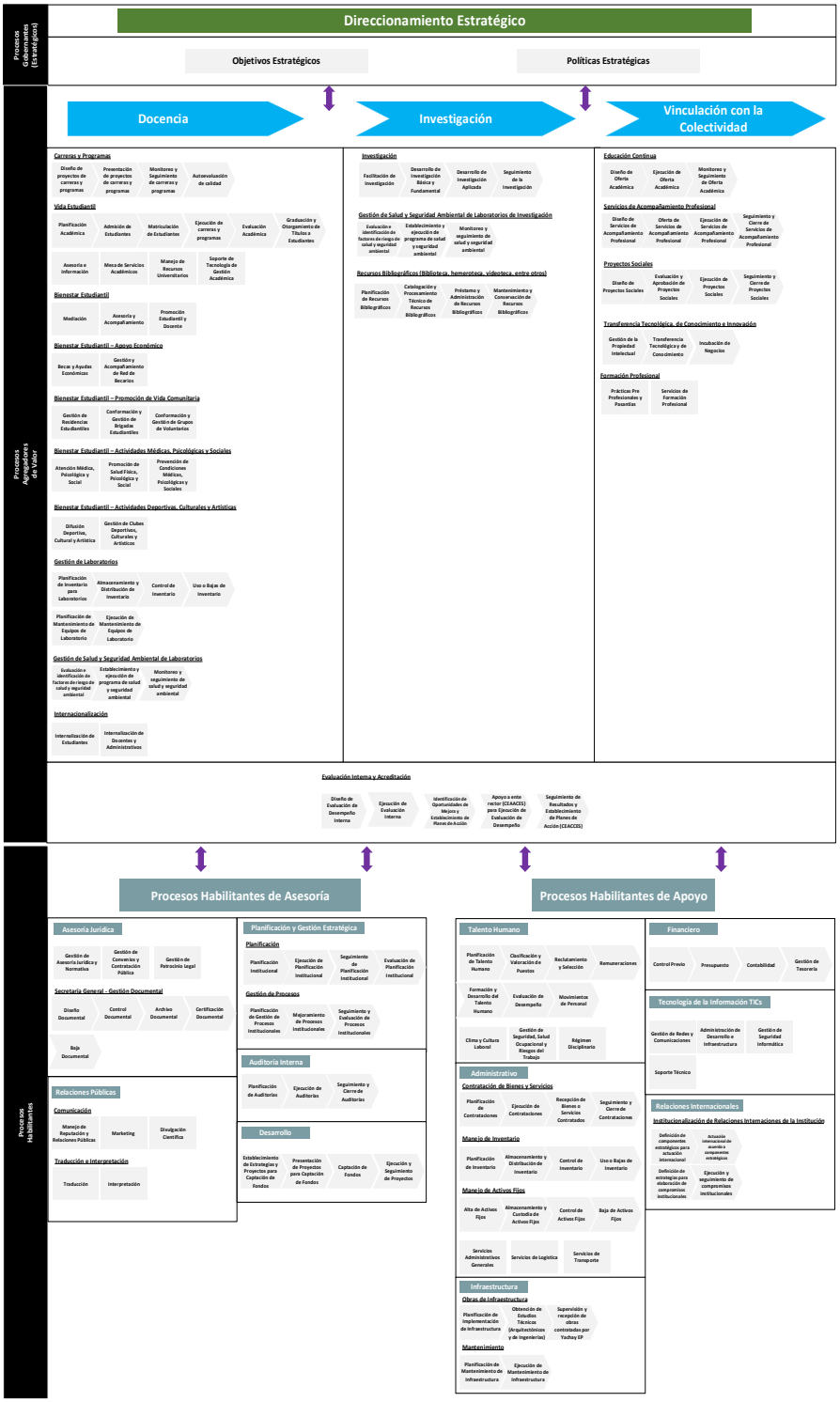

Gráfico 1: Mapa de Procesos de la Institución.

Orgánico – Funcional

1. Órganos de Dirección: Consejo Superior Universitario.
   a) Órganos Consultivos:
      - Consejo Académico
      - Consejo de Bienestar Universitario
      - Comité Consultivo de Graduados
   b) Instancias Asesoras al Órgano de Cogobierno:
      - Comisiones especializadas

2. Autoridades Ejecutivas:
   a. Rector
   b. Vicerrector Académico/Canciller

3. Unidades Administrativas de Apoyo subordinadas al Rectorado:
   a. Coordinación Administrativa Financiera;
   b. Coordinación de Desarrollo;
   c. Coordinación Jurídica;
   d. Coordinación de Talento Humano;
   e. Coordinación de Planificación y Gestión Estratégica;
   f. Coordinación de Infraestructura;
   g. Coordinación de Relaciones Públicas;
   h. Coordinación de Tecnologías de la Información; y,

4. Órganos subordinados al Vicerrectorado Académico/Cancillería

4.1. Unidades Académicas de Apoyo subordinados al Vicerrectorado Académico/Cancillería.

   a. Vicecancillería de Investigación, Tecnología e Innovación
      1. Coordinación de Biblioteca Académica
      2. Dirección de Cumplimiento de Investigación, Salud y Seguridad Ambiental.

   b. Vicecancillería de Asuntos Académicos
      1. Coordinación de Servicios Escolares
      2. Coordinación de Intercambio Académico
      3. Coordinación de Bienestar Estudiantil

5. Autoridades Académicas
    - Vicecancilleres
    - Decanos/as
    - Jefes de Departamento
    - Directores de Centros de Investigación

La responsabilidad sobre los temas de seguridad, recae en todas las áreas de la institución, pero, en especial en la Coordinación de Tecnologías de la Información, porque aquí, se administran las herramientas de seguridad informática existentes; se definen y establecen las políticas de seguridad a cumplir.

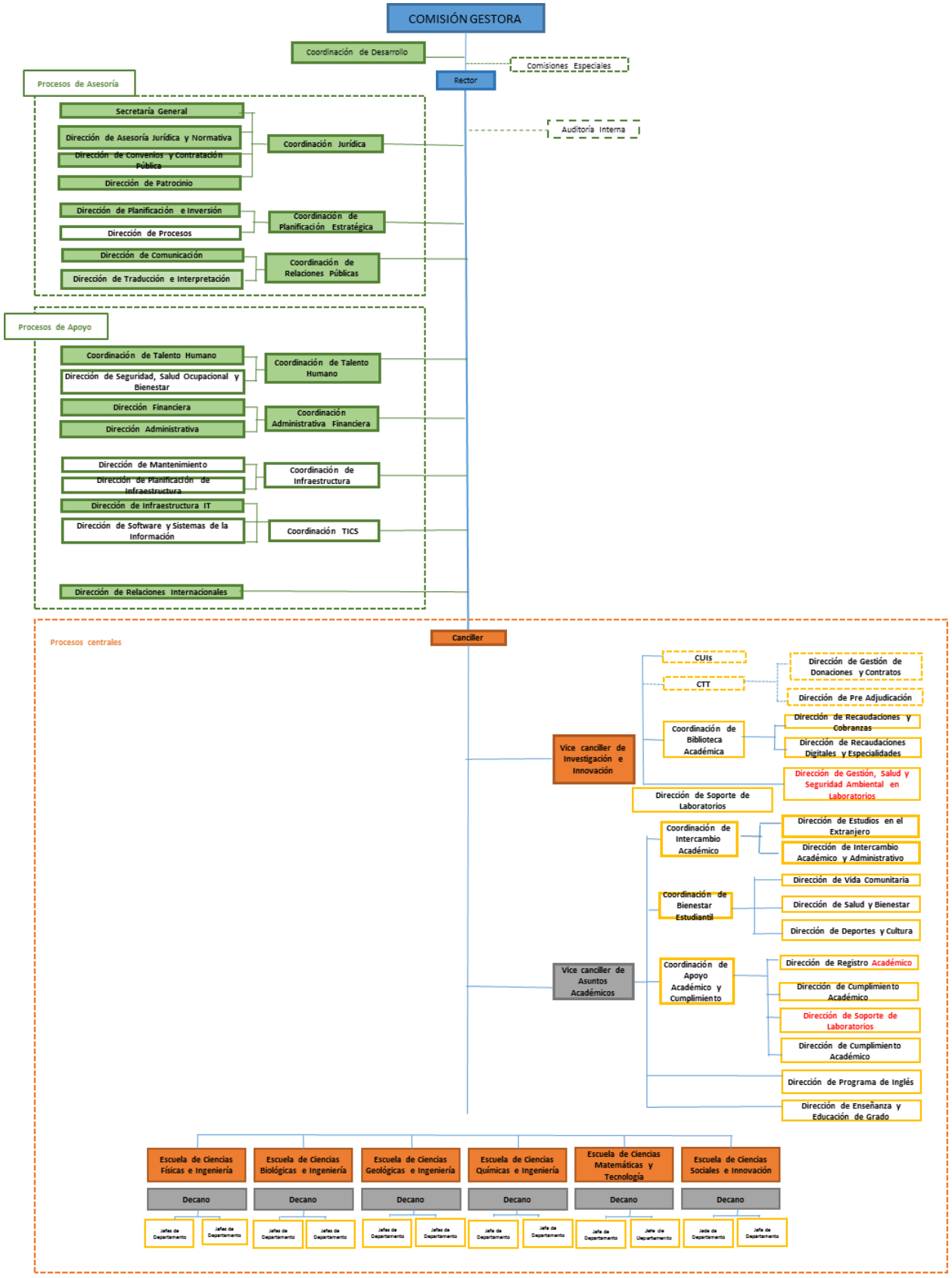
COMISIÓN GESTORA
Coordinación de Desarrollo
Comisiones Especiales
Rector
Auditoría Interna
Procesos de Asesoría
Secretaría General
Dirección de Asesoría Jurídica y Normativa
Dirección de Convenios y Contratación Pública
Dirección de Patrocinio
Coordinación Jurídica
Dirección de Planificación e Inversión
Dirección de Procesos
Coordinación de Planificación Estratégica
Dirección de Comunicación
Dirección de Traducción e Interpretación
Coordinación de Relaciones Públicas
Procesos de Apoyo
Coordinación de Talento Humano
Dirección de Seguridad, Salud Ocupacional y Bienestar
Coordinación de Talento Humano
Dirección Financiera
Dirección Administrativa
Coordinación Administrativa Financiera
Dirección de Mantenimiento
Dirección de Planificación de Infraestructura
Coordinación de Infraestructura
Dirección de Infraestructura IT
Dirección de Software y Sistemas de la Información
Coordinación TICS
Dirección de Relaciones Internacionales
Procesos centrales
Canciller
Vice canciller de Investigación e Innovación
CUIs
CTT
Dirección de Gestión de Donaciones y Contratos
Dirección de Pre Adjudicación
Coordinación de Biblioteca Académica
Dirección de Recaudaciones y Cobranzas
Dirección de Recaudaciones Digitales y Especialidades
Dirección de Gestión, Salud y Seguridad Ambiental en Laboratorios
Dirección de Soporte de Laboratorios
Vice canciller de Asuntos Académicos
Coordinación de Intercambio Académico
Dirección de Estudios en el Extranjero
Dirección de Intercambio Académico y Administrativo
Coordinación de Bienestar Estudiantil
Dirección de Vida Comunitaria
Dirección de Salud y Bienestar
Dirección de Deportes y Cultura
Coordinación de Apoyo Académico y Cumplimiento
Dirección de Registro Académico
Dirección de Cumplimiento Académico
Dirección de Soporte de Laboratorios
Dirección de Cumplimiento Académico
Dirección de Programa de Inglés
Dirección de Enseñanza y Educación de Grado
Escuela de Ciencias Físicas e Ingeniería
Escuela de Ciencias Biológicas e Ingeniería
Escuela de Ciencias Geológicas e Ingeniería
Escuela de Ciencias Químicas e Ingeniería
Escuela de Ciencias Matemáticas y Tecnología
Escuela de Ciencias Sociales e Innovación
Decano
Jefes de Departamento

Gráfico 2: Diagrama Organizacional

Área Física

Físicamente cuenta con un área de terreno de 4000 m2 aproximadamente y brinda servicios alojamiento a estudiantes, docentes e invitados del área academia, cuenta con varias áreas físicas llamadas: Hacienda San José, Ingenió San José, el Rosario, Residencias Patrimoniales y Bloques de Residencias; en las dos primeras áreas laboran personal académico y administrativo distribuidos de distinta manera, las demás áreas físicas son viviendas para residir a docentes, estudiantes e invitados académicos.

En cada área física cuenta con racks de comunicación, referente al data center este se encuentra ubicado de manera física y dividido: el primero en El Rosario y el segundo en la institución pública Corporación Nacional de Telecomunicaciones E.P., en esta última se tiene contratado un servicio de cloud computing, cada uno cumple con el estándar ANSI/TIA-942 y se clasifican con un TIER 1 y 3 respectivamente; los cuartos de rack de comunicación cuentan aire acondicionado y UPS. Adicional a esto se cuenta software como servicio en donde se tiene la plataforma de herramientas colaborativas (correo, almacenamiento, video llamadas, chat institucional), herramientas de desarrollo de sitios y clases virtuales.

Todas las zonas están protegidas con un sistema de control de acceso y cuenta con cámaras de vigilancia, para el acceso a las oficinas lo pueden realizar a través de tarjetas de proximidad, PIN y/o huella dactilar, para las residencias pueden acceder con huella dactilar. Para el ingreso al Data Center del Rosario, se accede con PIN y Tarjeta de proximidad, los usuarios autorizados son: el Administrador de Infraestructura de TI y Administrador de Redes.

Actualmente se maneja una topología de red mixta (estrella y distribuida) la misma que se representa en el siguiente gráfico:

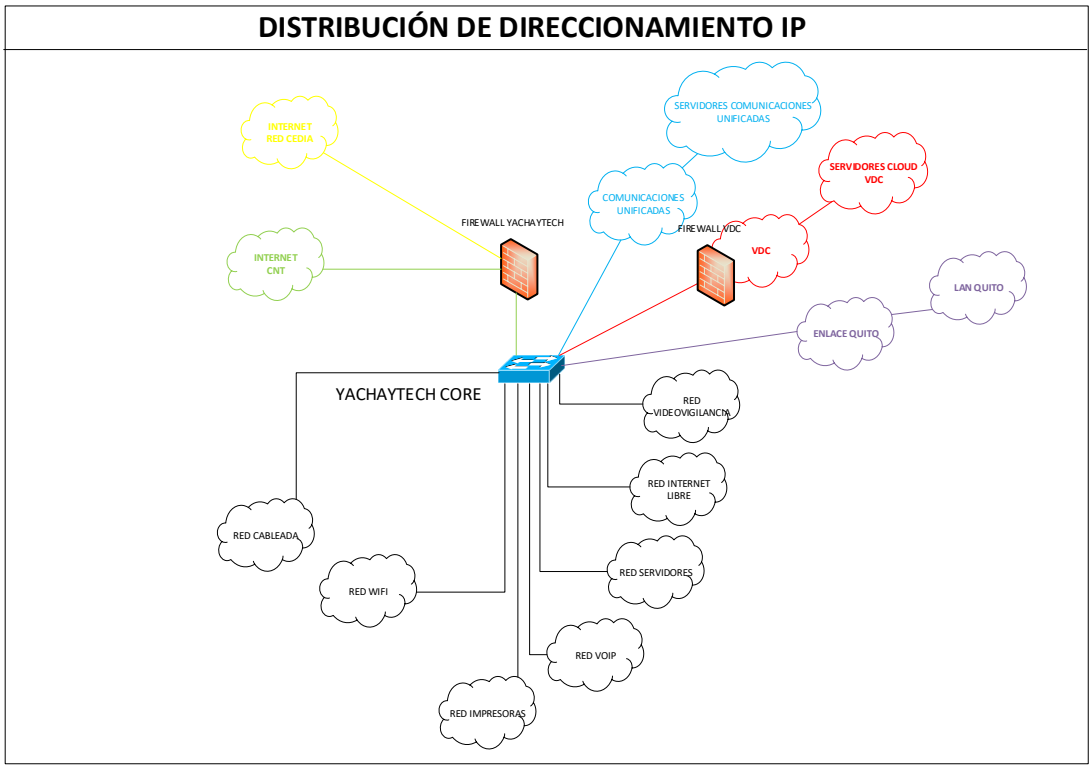

Gráfico 3: Diagrama de Red

La institución cuenta con varios Servicios de TI catalogados, los mismos que se detallan a continuación:

ITEM	SERVICIO	DESCRIPCIÓN DEL SERVICIO	CLIENTE	PRIORIDAD	PLATAFORMA/ PROVEEDOR
1	Google Apps	Comprende los servicios de correo electrónico, calendario, Classroom, Drive, Hanghuts, etc.	COMUNIDAD UNIVERSITARIA	1	Nube de Google
2	Quipux - Gestor Documental	Servicio brindado para el personal de la Universidad, envió y respuesta de documentos oficiales.	Todo el personal de la Universidad	1	Gobierno Electrónico
3	Impresoras / Escaner / Proyectores	El servicio se encarga de atender imprevistos o errores en el funcionamiento de las impresoras o escáner de la Universidad	COMUNIDAD UNIVERSITARIA	2	Soporte Técnico

4	Equipos de Computo	El servicio de soporte de equipos de cómputo se encarga de atender errores en cuanto al funcionamiento del equipo de computación (computador o laptop) asignado al servidor o servidora de la Universidad y funcionamiento de software	Todo el personal de la Universidad	1	Soporte Técnico
5	Ofimática	El servicio de Ofimática se encarga de solventar inconvenientes sobre la utilización o manejo de aplicaciones ofimáticas MS OFFICE (Word, Excel, Power Point, Outlook)	Todo el personal de la Universidad	1	Soporte Técnico
6	Software	Problemas con el funcionamiento del software instalado (Adobe Read, Java JRE, Bizage, Visio, Project, AutoCAD).	Todo el personal de la Universidad	2	Soporte Técnico
7	Antivirus	ESET ENDPOINT SECURITY	Todo el personal de la Universidad	2	Servidor Local
8	Internet	El servicio de soporte de internet se encarga de solventar errores o inconvenientes relacionados con la navegación en internet de acuerdo al perfil del funcionario y en los equipos autorizados	Todo el personal de la Universidad	1	Soporte Técnico / CNT
9	Internet Viviendas	El servicio de soporte de internet se encarga de solventar errores o inconvenientes relacionados con la navegación en Internet de las viviendas	Residencias	1	CNT
10	Sirha	Este servicio permite al usuario solicitar soporte cuando se presente problemas en el sistema de marcaciones de los funcionarios	Departamento de Talento Humano	1	Nube de CNT
11	ESIGEF	Servicio de un sistema de gestión y control financiero el mismo es administrado por el -Ministerio de Finanzas, si existe algún problema la Dir. de TIC's es el encargado de comunicar a las respectivas áreas de la Universidad	Todo el personal de la Universidad	1	Ministerio de Finanzas

12	Sistema Virtual de Aprendizaje - D2L	Sistema Virtual de Aprendizaje utilizado por la parte académica.	Docentes y Estudiantes	1	BrigthSpace
13	Comunicaciones Unificadas	Telefonía Ip, Videoconferencia - Webex, Telepresencia, etc.	Todo el personal de la Universidad	1	Nube de CNT
14	Servidor de Archivos	El servicio para compartir archivos como: rol de pagos, manuales, procedimientos, etc.	Todo el personal de la Universidad	3	Servidor Local
15	Funcionamiento Accesos Físicos	El servicio es respecto al normal funcionamiento de los accesos físicos a las áreas administrativas, residencias y aulas. Soyal y Suprema	COMUNIDAD UNIVERSITARIA	2	Soporte Técnico
16	Sistema de Reservaciones		Todo el personal de la Universidad	3	Nube de CNT
17	Servicio de Gestión Académico	Sistema ERP especializado en automatización de procesos tales como el registro del alumno, historial y programación académica, transferencias, administración de prerrequisitos, optimización de horarios (calendario maestro), definición de cupos de cursos, otras reglas de inscripción y procesos de becas institucionales y titulación. Además genera, publica y consulta de reportes, lo que permite un acceso inmediato a la información disponible para una toma de decisiones oportuna.	COMUNIDAD UNIVERSITARIA	1	Nube de CNT
18	Sistema de Bibliotecas	Sistema se encuentra funcionando en el denominado Koha es un sistema integrado de gestión de bibliotecas, el cual se destaca por ser el primero que se desarrolla en código fuente abierta.	COMUNIDAD UNIVERSITARIA	2	Nube de CNT
19	Sistema de Seguridad Perimetral	Sistema denominado cortafuego que bloquea el acceso remoto a determinados	COMUNIDAD	2	Servidor Local / Nube CNT

		puerto y permitiendo las conexiones que se han más seguras.	UNIVERSITARIA		
20	Sistema de Respaldos de Plataforma Virtual	Sistema que respalda y restaura máquinas virtuales, ayudando a mantener la disponibilidad de los Servicios de TI, cuando se presenta un evento.	COMUNIDAD UNIVERSITARIA	2	Servidor Local / Nube CNT
21	Sistema proxy de Consulta de Base de Datos Científicas	Sistema que se utiliza como herramienta de acceso remoto para la consulta de base de datos científicas.	COMUNIDAD UNIVERSITARIA	2	Servidor Local
22	Sistema de Monitoreo de Servicio de TI	Sistema de monitoreo del estado de los servidores y disponibilidad de la red LAN de la Institución	Departamento de TI	3	Servidor Local
23	Directorio Único	Sistema de autenticación de usuario único, el cual se	Todo el personal de la Universidad	1	Servidor Local
24	DHCP	Sistema de asignación de direcciones IP automático.	COMUNIDAD UNIVERSITARIA	2	Servidor Local
25	RADIUS	Sistema de control de acceso a la red LAN.	COMUNIDAD UNIVERSITARIA	2	Servidor Local
26	DNS	Sistema de resolución de dominios.	COMUNIDAD UNIVERSITARIA	2	Servidor Local
27	Sistema de inventario de HW ySW	Sistema de recolección de datos de Hardware y Software de Computadoras a través de agentes.	Departamento de TI	3	Servidor Local
28	Sistema de Mesa de Servicio	Sistema de automatización del proceso de Mesa de Ayuda para los servicios de TI.	COMUNIDAD UNIVERSITARIA	2	Servidor Local
29	Autoservicio de Cuenta Única	Sistema Self-Service de contraseña, el mismo sirve para recuperar y cambiar contraseña de una única cuenta.	COMUNIDAD UNIVERSITARIA	2	Servidor Local

30	Sistema de cola de impresión	Sistema de impresión única y despliega las impresiones con control del usuario.	COMUNIDAD UNIVERSITARIA	2	Servidor Local
31	Sistema de Facturación y Anexos Transaccionales (SITAC)	SITAC Plus tiene la posibilidad de emitir documentos electrónicos en línea autorizados por el Servicio de Rentas Internas y con 37 dígitos para la autorización. Genera Anexo Transaccional Simplificado (ATS) y Anexo de Retenciones en la Fuente de Impuesto a la Renta por Otros Conceptos (REOC) No requiere validador del SRI. Archivos de declaraciones de los formularios 103 y 104 para enviar por Internet (DIMM). Toda la información es tomada del sistema automáticamente sin procesos adicionales de integración con otros programas. Evita que el SRI le notifique por diferencias e inconsistencias entre anexos y formularios ya que todo se genera desde el mismo sistema, todo a la vez está cuadrado con la contabilidad	Coordinación Administrativa Financiera	2	Nube CNT
32	Sistema de Actualización de Windows	Sistema que centraliza las actualizaciones de los paquetes de Microsoft y los distribuye de acuerdo a la criticidad.	COMUNIDAD UNIVERSITARIA	3	Servidor Local

Cuadro 1: Servicios de TIC.

1.5 Objetivos del Plan Director

Como se ha comentado con anterioridad, el Plan Director de Seguridad en sí mismo no tiene interés, ha de ir alineado con un objetivo estratégico que es el que va a delimitar el alcance del Plan Director de Seguridad.

En nuestro caso concreto, el alcance del Plan Director de Seguridad se va a enmarcar dentro de los principios y objetivos establecidos en el estatuto de institución, de los cuales describimos a continuación:

- Principio de “Calidad.- La Universidad se regirá por los máximos estándares de excelencia en sus actividades y programas académicos, a fin de asegurar el mejoramiento continuo en todos sus niveles de formación, capacitación e investigación”
- Objetivo de “Los demás objetivos establecidos para la educación superior en la constitución de la República del Ecuador, la Ley Orgánica de Educación Superior, su Reglamento, el presente Estatuto y demás normativa aplicable”.

Basados en el objetivo institucional anteriormente citado podemos establecer que la entidad debe considerar:

Que, el numeral 2 del artículo 16 de la Constitución de la República del Ecuador establece como derecho de las personas, en forma individual o colectiva, el acceso universal a las tecnologías de información y comunicación;

Que, el numeral 21 del artículo 66 de la Constitución de la República del Ecuador reconoce y garantiza a las personas el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; derecho que protege cualquier otro tipo o forma de comunicación;

Que, el artículo 77 de la Ley Orgánica de la Contraloría General del Estado establece la obligación del Titular de la entidad de dirigir y asegurar la implantación, funcionamiento y actualización de los sistemas administrativos;

Que, el artículo 2 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos reconoce y otorga igual valor jurídico a los mensajes de datos que a los documentos físicos;

Que, el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, artículo 148 y Disposición Transitoria Décima Tercera, determina a las entidades contratantes del sector público orden de prelación en la contratación pública relacionada a software y un plan de migración a software libre;

Que, el Reglamento General para la administración, utilización, manejo y control de los bienes y existencias del sector público, considera, en su artículo 4, la reglamentación interna para la

administración, uso, control y destino de los bienes del Estado; y en los artículos 103 y 104, disposiciones para el registro y mantenimiento de equipos informáticos, hardware y software;

Que, las Normas de Control Interno de la Contraloría General del Estado, Grupo 410 Tecnologías de la Información y Grupo 500 Información y Comunicación, regulan la información y la comunicación y su soporte tecnológico informático, con necesaria referencia a un modelo de información de la organización que facilite la creación, uso y compartición de la misma y garantice su disponibilidad, integridad, exactitud y seguridad, sobre la base de la definición e implantación de los procesos y procedimientos correspondientes;

Que, la Norma de Control Interno 410-04 Políticas y procedimientos, determina a la Unidad de Tecnología de Información definir, documentar y difundir políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, considerándose temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información; así mismo, la incorporación de controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos; y, la implantación de procedimientos de supervisión de las funciones de tecnología de información;

Que, la Norma de Control Interno 300-03 Valoración de los riesgos, determina "Se consideran factores de alto riesgo potencial los programas o actividades complejas... sistemas de información rediseñados... nueva tecnología, entre otros. La valoración del riesgo se realiza usando el juicio profesional y la experiencia";

Se trata de un objetivo amplio que requiere la revisión de todos los sistemas de la institución y determinar qué puntos débiles existen en cada uno de ellos y realizar propuestas de mejoras puntuales y continuas.

Objetivo General

Definir un plan director de seguridad de la información que esté acorde con los lineamientos generales que la institución educativa debe seguir para garantizar la protección y el buen uso de la información y los sistemas de información que la entidad utiliza.

Objetivos específicos

- 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.

1.6 Alcance

El plan director de seguridad es una hoja de ruta que debe seguir la institución para conseguir gestionar de forma adecuada la seguridad, para la definición del plan director de seguridad se deberán contemplar los siguientes objetivos:

1. Garantizar la confidencialidad, integridad y disponibilidad de la información de los estudiantes en los sistemas de información que capturen, transmitan, almacenen y/o procesen dicha información.
2. Establecer de manera clara los requisitos de seguridad de la información que la institución debe cumplir con el fin de garantizar la protección de la información de las diferentes amenazas a las que está expuesta, minimizando los riesgos, con el fin de cumplir con sus obligaciones para con los estudiantes, docentes, personal administrativo, autoridades y colaboradores; garantizando con ello la continuidad del negocio.
3. Realizar un análisis diferencial del estado actual del estado de seguridad de los activos de la compañía, versus el cumplimiento de la norma ISO/IEC 27001 e ISO/IEC 27002, para que a partir de este análisis se identifiquen los recursos necesarios y se puedan establecer los planes de trabajo con el fin de cumplir las normas.

Se define para el alcance de la implementación del SGSI, los procesos medulares que se encuentran dentro de los Procesos Agregado de Valor (Ver gráfico 1) de docencia, los mismos que son:

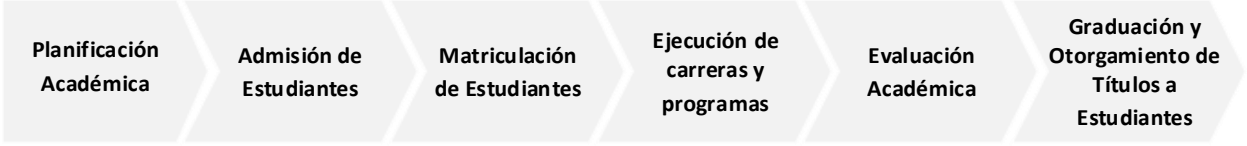

Gráfico 4: Procesos Agregado de Valor para el SGSI.

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 (Ver gráfico 4) 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.

1.7 Análisis Diferencial

A continuación, se realiza el análisis inicial de los documentos mínimos y registros que se debe tener para cumplir con la ISO 27001:2013, adicional, se revisara todos los objetivos de control y controles estipulados por la normativa ISO 27002:2013:

Documentos para la ISO 27001:2013

Documentos*	Capítulo de ISO 27001:2013	Nivel de Cumplimiento (%)
Alcance del SGSI	4.3	**0%**
Políticas y objetivos de seguridad de la información	5.2, 6.2	**0%**
Metodología de evaluación y tratamiento de riesgos	6.1.2	**0%**
Declaración de aplicabilidad	6.1.3 d)	**0%**
Plan de tratamiento del riesgo	6.1.3 e), 6.2	**0%**
Informe sobre evaluación y tratamiento de riesgos	8.2, 8.3	**0%**
Definición de funciones y responsabilidades de seguridad	A.7.1.2, A.13.2.4	**20%**

Inventario de activos	A .8.1 .1	**80%**
Uso aceptable de los activos	A .8.1 .3	**0%**
Política de control de acceso	A .9.1.1	**0%**
Procedimientos operativos para gestión de TI	A .12.1.1	**20%**
Principios de ingeniería para sistema seguro	A .14.2.5	**0%**
Política de seguridad para proveedores	A .15.1.1	**0%**
Procedimiento para gestión de incidentes	A .16.1.5	**0%**
Procedimientos de la continuidad del negocio	A .17 .1.2	**0%**
Requisitos legales, normativos y contractuales	A .18.1.1	**20%**

Cuadro 2: Documentos básicos para la Certificación ISO 27001:2013.

Registros para la ISO 27001:2013

Registros*	Capítulo de ISO 27001:2013	Nivel de Cumplimiento (%)
Registros de capacitación, habilidades, experiencia y calificaciones	7.2	**0%**
Resultados de supervisión y medición	9.1	**0%**
Programa de auditoría interna	9.2	**0%**
Resultados de las auditorías internas	9.2	**0%**
Resultados de la revisión por parte de la dirección	9.3	**0%**
Resultados de acciones correctivas	10.1	**0%**
Registros sobre actividades de los usuarios, excepciones y eventos de	A .12.4.1, A .12.4.3	**0%**

Cuadro 3: Registros básicos para la Certificación ISO 27001:2013.

*Se pueden excluir los controles del Anexo A si la institución determina que no existen riesgos ni otros requisitos que podrían demandar la implementación de un control.

A continuación, se realiza el análisis inicial de todos los objetivos de control estipulados por la normativa ISO 27002:2013, para más detalle ver el ANEXO I:

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%**

Cuadro 4: Tabla de Cumplimiento Inicial ISO 27002:2013.

1.8 Resultado

Como se puede evidenciar en el Análisis Diferencial entre los requisitos para certificar con la ISO 27001:2013 y el cumplimiento de los objetivos de control de la ISO 27002:2013, se puede establecer que se tiene aspectos trabajados de forma empírica más no formal, el personal técnico de la institución tiene experiencia y en algunos casos tienen capacitaciones respecto a la seguridad informática por lo que tiene concientización de los aspectos de seguridad básicos, respecto al personal jerárquico superior se observó que tienen conocimiento sobre la seguridad de una forma global ya que se han enterado de forma informal; por medio de la prensa y televisión; y en redes sociales.

A continuación, se presenta los gráficos de tipo de radar en donde se puede establecer el nivel de cumplimiento por cada norma:

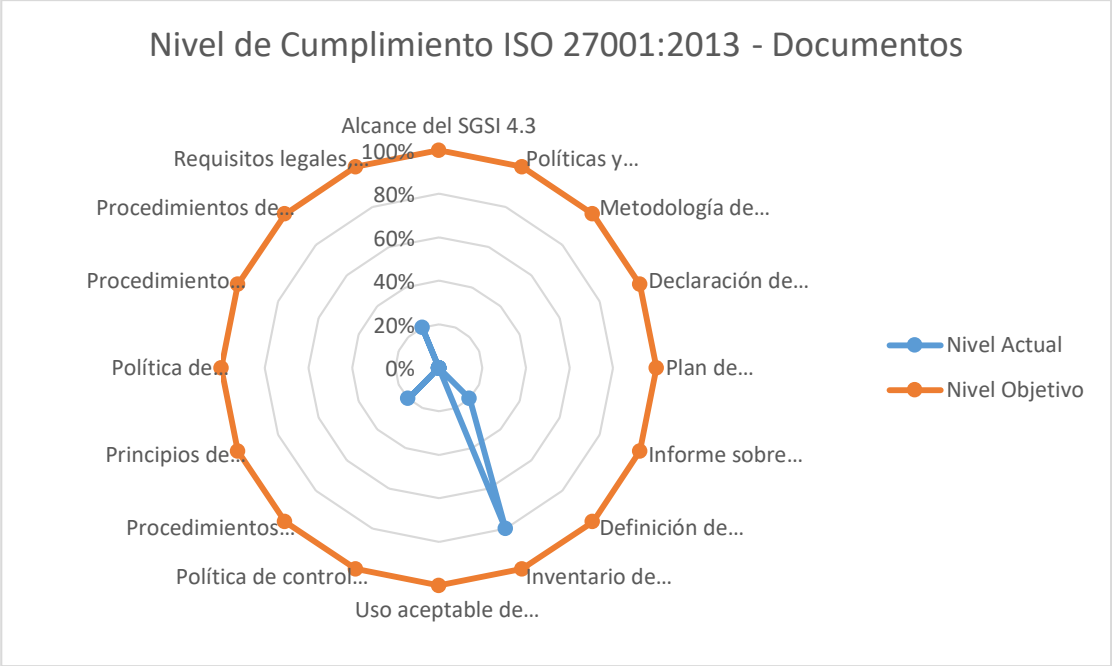

Gráfico 5: Nivel de Cumplimiento ISO 27001:2013 - Documentos

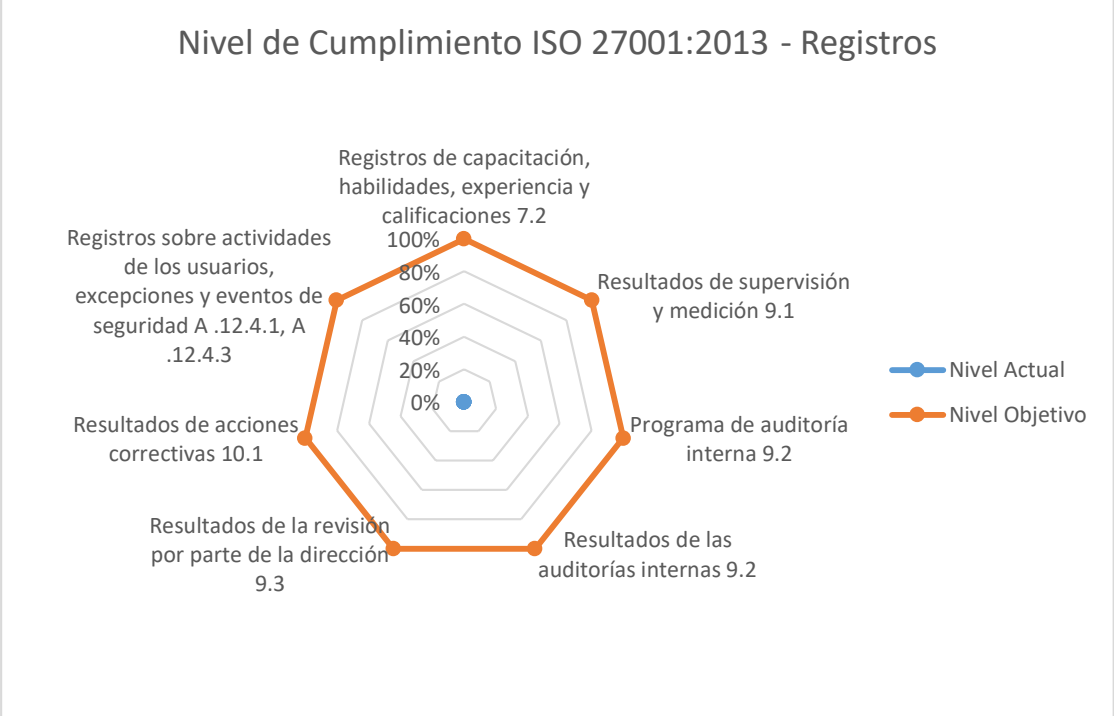

Gráfico 6: Nivel de Cumplimiento ISO 27001:2013 - Registros

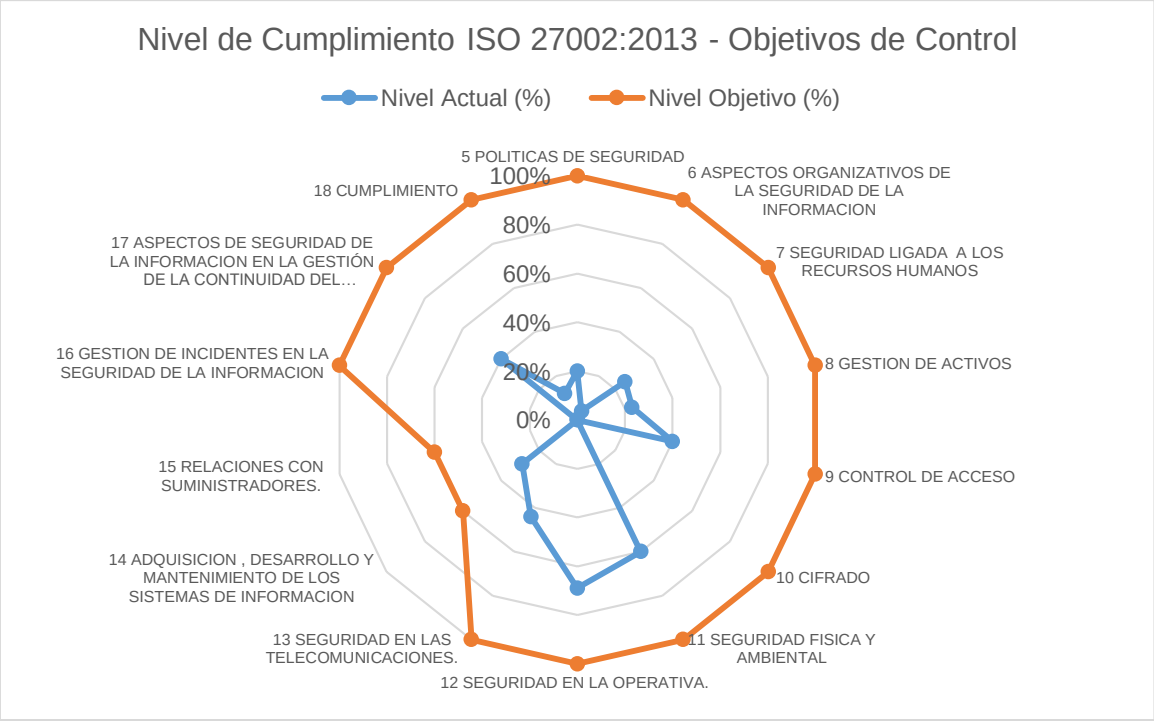

Gráfico 7: Nivel de Cumplimiento ISO 27002:2013 – Objetivos de Control

2 Sistema de Gestión Documental

2.1 Introducción

Los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo, para el presente Sistema de Gestión de Seguridad de la Información se define el esquema documental establecidos en la norma ISO/IEC 27001 como necesarios para una certificación del sistema.

2.2 Esquema Documental

De acuerdo a la ISO/IEC 27001 se define los documentos necesarios para poder certificar el sistema, el presente proyecto se centrará en los siguientes:

2.2.1 **Política de Seguridad**:

La institución actualmente contempla en temas de seguridad políticas de navegación web para todos sus usuarios para lo cual es una para de la normativa interna que debe conocer y cumplir todo el personal afectado. El contenido de la Política debe cubrir más aspectos del mencionado y que están relacionados al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, etc. Ver ANEXO V

2.2.2 **Procedimiento de Auditorías Internas:**

Dentro de la estructura organizacional de la institución actual no se contempla un área de auditoria interna de acuerdo a nuestra propuesta esta área debe ser considerada entre las unidades Administrativas de Apoyo subordinadas al Rectorado, es imprescindible implementar un proceso de auditoría interna para realizar un correcto mantenimiento continuado y evolutivo del Sistema de Gestión de la Seguridad de la Información. Mediante estas auditorías internas se realiza una mejora del sistema a partir de la implementación inicial. Ver ANEXO VI.

2.2.3 **Gestión de Indicadores:**

Para gestionar indicadores estos deben ser creados orientados principalmente en la medición de la eficacia, eficiencia y efectividad de los componentes que se encuentran definidos en el modelo del sistema de gestión de seguridad de la información, estos

indicadores deben servir de insumo para los componentes de mejora continua, permitiendo adoptar decisiones de mejora. Ver ANEXO VII.

2.2.4 **Procedimiento Revisión por Dirección:**

La Dirección de la institución debe realizar revisiones periódicas en los aspectos más importantes que han ocurrido con relación al SGSI. Para esta revisión la normas ISO 27001:2013 establece los puntos de entrada y salida.

Para tener más detalle del procedimiento de revisión revisar el ANEXO VIII

2.2.5 **Gestión de Roles y Responsabilidades:**

En toda la Gestión de la Seguridad de la información debe existir una representación definida por la dirección responsable de desarrollar, evaluar y revisar la Política de Seguridad de la información de la institución. Esta representación, en función de la envergadura de la organización, puede ser asumida por un rol existente o, en el caso de organizaciones con cierto volumen y/o relevancia, puede ser un rol único y especifico. Esta representación recibe el nombre de Responsable u Oficial de Seguridad de la información, Director de Seguridad de la Información o, en inglés, CISO (Chief Information Security Officer).

La descripción de los roles y responsabilidades mencionadas se encuentran detallados en el ANEXO IX.

2.2.6 **Metodología de Análisis de Riesgos:**

El análisis de riesgos, como pueden ser la pérdida de confidencialidad, integridad o disponibilidad de los activos de la empresa ha de seguir una metodología que define los criterios que influyen en el riesgo global, escalas de impacto, criterios de aceptación de riesgo y tipos de impacto, entre otros elementos a analizar.

La metodología a utilizar para el análisis de riesgos es Magerit V3. Se trata de una metodología muy utilizada en España y parte de Iberoamérica que tiene la particularidad de expresar sus resultados en términos cuantitativos o cualitativos con lo que facilita la toma de decisión, en el presente estudio se expresará los resultados en términos cualitativos.

Para tener detalles de la metodología utilizada ver el ANEXO X.

2.2.7 **Declaración de Aplicabilidad:**

En la normativa ISO 27001 se establece que la aplicabilidad de los controles puede deberse por una obligación contractual, por un requerimiento regulatorio o por un requerimiento del negocio. De la misma manera, se estipula que alguno de los controles puede ser excluido de la aplicabilidad de la norma. En el caso concreto de la institución objeto de este estudio la mayoría de controles son aplicables.

En el ANEXO XI, se tiene la matriz de aplicabilidad.

3 Análisis de Riesgos

3.1 Introducción

Antes de realizar una propuesta de proyectos a implementar en la institución para mitigar ciertas amenazas o riesgos, primero es necesario el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir.
A continuación, se detalla el análisis de los activos de la empresa, los riesgos asociados y el impacto potencial sobre los activos, hacia la consecución del Plan de Implementación de un SGSI, a partir de la metodología definida en el punto “2.2.6. Metodología de Análisis de Riesgos”, ver ANEXO X.

3.2 Inventario de activos

Nuestro primer punto para el análisis es analizar los activos vinculados a la información y que interviene dentro de los Servicios de TI que intervienen en los procesos seleccionados en el numeral “1.6 Alcance”. Es habitual agrupar los activos por grupos.

En nuestro caso, podemos agrupar los activos en grupos acordes con la metodología MAGERIT. Nos centraremos en:

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

Los resultados del inventario deberían recogerse en tablas para su posterior estudio. Estas tablas podrían tener una estructura tan simple como en grupo al que pertenece el activo y el activo en sí.

Item	Ámbito	Activo	Cantidad	Ubicación
1	Instalaciones	Data Center	1	El Rosario
2	Instalaciones	Cuarto de Rack	1	San José
3	Instalaciones	Cuarto de Rack	1	Ingenio - Principal
4	Instalaciones	Cuarto de Rack	1	Ingenio - Biblioteca
5	Instalaciones	Cuarto de Rack	1	Ingenio - Aulas
6	Red	Puntos de Red – Cableado Estructurado – Servidores	7	El Rosario
7	Red	Puntos de Red – Cableado Estructurado – Puestos de Trabajo	88	San José

8	Red	Puntos de Red – Cableado Estructurado – Puestos de Trabajo	20	Ingenio
9	Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red	7	El Rosario
10	Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red	56	San José
11	Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red	49	Ingenio
12	Red	Switch Core	2	El Rosario
13	Red	Switch 24 puertos	3	El Rosario
14	Red	Switch 24 puertos	4	Ingenio
15	Red	Switch 48 puertos	16	El Rosario - Residencias
16	Red	Switch 48 puertos	6	San José
17	Red	Switch 48 puertos	10	Ingenio
18	Red	Access Point	1	El Rosario
19	Red	Access Point	13	San José
20	Red	Access Point	17	Ingenio
21	Red	Routers Inalambricos	1	El Rosario
22	Red	Routers Inalambricos	6	San José
23	Red	Routers Inalambricos	4	Ingenio
24	Red	Firewall	2	El Rosario
25	Red	Routers	2	El Rosario
26	Hardware	Computadores de Escritorio	23	San José - Ingenio
27	Hardware	Computadores Todo en Uno	17	Ingenio
28	Hardware	Portátiles	262	San José - Ingenio
29	Hardware	Apple MAC	4	San José
30	Hardware	Impresoras	3	El Rosario
31	Hardware	Impresoras	7	El Ingenio
32	Hardware	Impresoras	12	San José
33	Hardware	Teléfonos IP	3	El Rosario
34	Hardware	Teléfonos IP	25	San José
35	Hardware	Teléfonos IP	9	Ingenio
36	Hardware	Lectores de tarjetas de proximidad	5	El Rosario
37	Hardware	Lectores de tarjetas de proximidad	17	San José
38	Hardware	Lectores de tarjetas de proximidad	22	El Ingenio (Aulas, Biblioteca, Administrativo)

39	Hardware	Servidores	6	El Rosario
40	Hardware	NAS	1	El Rosario
41	Software	Ofimática	312	Toda la Institución
42	Software	Sistema Operativo Cliente	312	Toda la Institución
43	Software	Motor de Base de Datos	2	Servicios de Gestión
44	Software	Sistema Operativo Servidores	24	Toda la Institución
45	Software	Licencia de Escritorio	50	Servicios de Gestión
46	Software	Aplicaciones de Desarrollo	2	Servicios de Gestión
47	Software	Servidor de Terminal	2	Servicios de Gestión
48	Software	Servidor Directorio Activo	2	Toda la Institución
49	Software	Servidor de Aplicaciones	2	Servicios de Gestión
50	Software	Licencia de Antivirus Clientes	500	Toda la Institución
51	Software	Servidor DHCP	1	Toda la Institución
52	Software	Servidor Antivirus	1	Toda la Institución
53	Software	Servidor de Backup MV	1	Toda la Institución
54	Software	Servidor de Backup	1	Servicios de Gestión
55	Datos	Base de Datos Estudiantes	1	Servicios de Gestión
56	Datos	Base de Datos Docentes	1	Servicios de Gestión
57	Datos	Base de Datos Personal Administrativo	1	Toda la Institución
58	Personal	Estudiantes	761	Toda la Institución
59	Personal	Docentes	126	Toda la Institución
60	Personal	Personal Administrativo	165	Toda la Institución
61	Personal	Administrador de Infraestructura	1	Toda la Institución
62	Personal	Administrador Base de Datos	1	Toda la Institución
63	Servicios	Correo Electrónico	1	Google Suite
64	Servicios	Herramienta Colaborativa	1	Google Suite
65	Servicios	IaaS	1	CNT
66	Servicios	Sistema Académico	1	Power Campus Front End
67	Servicios	Sistema Académico	1	Power Campus Back End
68	Servicios	Sistema Virtual de Aprendizaje	1	D2L Front End
69	Servicios	Sistema Virtual de Aprendizaje	1	D2L Back End
70	Servicios	Usuario Externo	1	
71	Servicios	Usuario Interno	1	

Cuadro 5: Inventario de Activos

3.3 Valoración de los activos

Si pensamos en el proceso en conjunto, el objetivo final es tomar un conjunto de medidas que garanticen nuestros activos. El sentido común indica que el coste de las medidas no deberá ser superior al coste del activo protegido. Empezaremos por tanto por determinar el valor de los diferentes activos.

3.4 Dimensiones de seguridad

Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos debe indicarse cuál es el aspecto de la seguridad más crítico. Esto será de ayuda en el momento de pensar en posibles salvaguardas, ya que estas se enfocarán en los aspectos que más nos interesen.

Una vez identificados los activos, debe realizarse la valoración ACIDA de los mismos. Dicha valoración viene a medir la criticidad en las cinco dimensiones de la seguridad de la información manejada por el proceso de negocio. Esta valoración nos permitirá a posteriori valorar el impacto que tendrá la materialización de una amenaza sobre la parte de activo expuesto (no cubierto por las salvaguardas en cada una de las dimensiones).

El valor que reciba un activo puede ser propio o acumulado. El valor propio se asignará a la información, quedando los demás activos subordinados a las necesidades de explotación y protección de la información. Así pues, los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos. Cada activo de información puede poseer un valor diferente en cada una de las diferentes dimensiones para la organización que deseemos analizar. Para ello hemos de tener presente siempre que representa cada dimensión.

Una vez explicadas las cinco dimensiones se ha de tener presente la escala en la que se realizarán las valoraciones (Ver Anexo X).

A la hora de realizar las ponderaciones para cada activo se ha de tener presente la importancia o participación del activo en la cadena de valor del servicio, evitando inconformidades del tipo “todo es muy importante” y obligando así al o a los responsables de realizar dicha valoración a discernir entre lo que es realmente importante y lo que no lo es tanto.

Se valorarán los activos como de importancia “Muy Alta”, “Alta”, “Media”, “Baja” o “Despreciable” a la vez que se le asignará a cada activo en cada dimensión una valoración del [0-10].

3.5 Tabla resumen de valoración

De forma resumida, lo visto hasta ahora nos debe permitir generar una tabla donde reflejaremos tanto la valoración de activos como los aspectos críticos del mismo. A la tabla resultante la llamaremos Valoración de los activos.

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
Red	Switch 48 puertos - San José	MEDIA	8	8	8	8	8
Red	Switch 48 puertos – Ingenio	MEDIA	8	8	8	8	8
Red	Access Point - El Rosario	BAJA	6	5	5	5	5
Red	Access Point - San José	BAJA	6	5	5	5	5
Red	Access Point – Ingenio	BAJA	6	5	5	5	5
Red	Routers Inalambricos - El Rosario	BAJA	6	5	5	5	5
Red	Routers Inalambricos - San José	BAJA	6	5	5	5	5
Red	Routers Inalambricos – Ingenio	BAJA	6	5	5	5	5
Red	Firewall - El Rosario	MUY ALTA	10	8	6	10	8
Red	Routers - El Rosario	ALTA	6	6	4	10	6

Hardware	Computadores de Escritorio - San José – Ingenio	BAJA	2	8	8	4	8
Hardware	Computadores Todo en Uno - Ingenio	DESPRECIABLE	2	8	8	4	8
Hardware	Portátiles - San José – Ingenio	BAJA	2	8	8	4	8
Hardware	Apple MAC - San José	DESPRECIABLE	2	8	8	4	8
Hardware	Impresoras - El Rosario	MEDIA	2	8	4	4	8
Hardware	Impresoras - El Ingenio	MEDIA	2	8	4	4	8
Hardware	Impresoras - San José	MEDIA	2	8	4	4	8
Hardware	Teléfonos IP - El Rosario	BAJA	2	8	4	4	8
Hardware	Teléfonos IP - San José	BAJA	2	8	4	4	8
Hardware	Teléfonos IP – Ingenio	BAJA	2	8	4	4	8
Hardware	Lectores de tarjetas de proximidad - El Rosario	ALTA	8	8	8	8	8
Hardware	Lectores de tarjetas de proximidad - San José	ALTA	4	4	4	4	4
Hardware	Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	ALTA	4	4	4	4	4
Hardware	Servidores - El Rosario	ALTA	8	8	8	10	8
Hardware	NAS - El Rosario	BAJA	4	4	4	4	4
Software	Ofimática - Toda la Institución	BAJA	4	8	6	6	4
Software	Sistema Operativo Cliente - Toda la Institución	BAJA	4	8	6	10	4
Software	Motor de Base de Datos - Servicios de Gestión Académica.	MUY ALTO	8	10	8	10	8
Software	Sistema Operativo Servidores - Toda la Institución	MEDIA	10	8	8	10	8
Software	Licencia de Escritorio Remoto - Dispositivo - Servicios de Gestión Académica.	MEDIA	10	8	8	10	8
Software	Aplicaciones de Desarrollo - Servicios de Gestión Académica.	MEDIA	10	8	8	8	8
Software	Servidor de Terminal Services - Servicios de Gestión Académica.	MEDIA	8	6	6	10	10
Software	Servidor Directorio Activo - Toda la Institución	MUY ALTA	10	8	6	10	10
Software	Servidor de Aplicaciones - Servicios de Gestión Académica.	ALTA	6	6	4	8	6
Software	Licencia de Antivirus Clientes - Toda la Institución	MEDIA	6	8	6	6	8
Software	Servidor DHCP - Toda la Institución	ALTA	6	6	6	10	10
Software	Servidor Antivirus - Toda la Institución	MEDIA	6	8	6	6	8
Software	Servidor de Backup MV - Toda la Institución	ALTA	4	8	6	6	6

Software	Servidor de Backup Archivos - Servicios de Gestión Académica.	MUY ALTA	6	8	6	8	6
Datos	Base de Datos Estudiantes - Servicios de Gestión Académica.	MUY ALTA	8	10	10	10	8
Datos	Base de Datos Docentes - Servicios de Gestión Académica.	MUY ALTA	8	10	10	10	8
Datos	Base de Datos Personal Administrativo - Toda la Institución	MUY ALTA	8	10	10	10	8
Personal	Estudiantes - Toda la Institución	ALTA	6	8	6	8	6
Personal	Docentes - Toda la Institución	ALTA	6	8	6	8	6
Personal	Personal Administrativo - Toda la Institución	MEDIA	6	8	6	8	6
Personal	Administrador de Infraestructura - Toda la Institución	ALTA	8	8	6	10	10
Personal	Administrador Base de Datos - Toda la Institución	ALTA	8	10	10	10	10
Servicios	Correo Electrónico - Google Suite	MEDIA	8	4	4	8	8
Servicios	Herramienta Colaborativa - Google Suite	BAJA	8	6	6	10	8
Servicios	IaaS – CNT	MUY ALTA	8	10	10	10	10
Servicios	Sistema Académico - Power Campus	MUY ALTA	8	6	6	10	8
Servicios	Sistema Virtual de Aprendizaje - D2L	MUY ALTA	8	6	6	10	8
Servicios	Usuario Externo -	MEDIA	8	8	6	6	6
Servicios	Usuario Interno -	MUY ALTA	8	6	6	10	8

Cuadro 6: Tabla de valoración de activos

3.6 Análisis de Amenazas

Los activos están expuestos a amenazas y estas pueden afectar a los distintos aspectos de la seguridad. A nivel metodológico, queremos analizar qué amenazas pueden afectar a qué activos. Una vez estudiado, estimar cuán vulnerable es el activo a la materialización de la amenaza, así como la frecuencia estimada de la misma.

Lo más habitual en un enfoque metodológico es disponer de una tabla inicial de amenazas. En nuestro caso, y por un tema de homogeneidad, utilizaremos también las usadas en MAGERIT V3.

La información recopilada debe dar lugar a una tabla resumen como la que se muestra en la tabla 6 para un activo determinado. En definitiva, para cada tipo de activo se analizará la frecuencia (Ver ANEXO X) con que puede producirse la amenaza, así como su impacto en las distintas dimensiones de la seguridad del activo.

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%
Instalaciones	Cuarto de Rack - Ingenio - Biblioteca	[I.6]	PR-B	0%	0%	0%	100%	0%
Instalaciones	Cuarto de Rack - Ingenio - Aulas	[N.*]	PR-MB	0%	0%	0%	100%	0%
Instalaciones	Cuarto de Rack - Ingenio - Aulas	[I.*]	PR-MB	0%	0%	0%	100%	0%
Instalaciones	Cuarto de Rack - Ingenio - Aulas	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[E.25]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[A.12]	PR-B	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[N.*]	PR-MB	0%	0%	0%	100%	0%

Red	Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[E.25]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[A.12]	PR-B	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Puestos de Trabajo – Ingenio	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Puestos de Trabajo - Ingenio	[E.25]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Puestos de Trabajo - Ingenio	[A.12]	PR-B	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[E.25]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[A.14]	PR-B	80%	100%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[E.25]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[A.14]	PR-B	80%	100%	0%	100%	0%

Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - Ingenio	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - Ingenio	[E.25]	PR-MB	0%	0%	0%	100%	0%
Red	Puntos de Red – Cableado Estructurado – Dispositivos de Red - Ingenio	[A.14]	PR-B	80%	100%	0%	100%	0%
Red	Switch Core - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Switch Core - El Rosario	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Switch Core - El Rosario	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Switch Core - El Rosario	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Switch Core - El Rosario	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Switch 24 puertos - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Switch 24 puertos - El Rosario	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Switch 24 puertos - El Rosario	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Switch 24 puertos - El Rosario	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Switch 24 puertos - El Rosario	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Switch 24 puertos - Ingenio	[N.*]	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	Switch 48 puertos - San José	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Switch 48 puertos - San José	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Switch 48 puertos - San José	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Switch 48 puertos - San José	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Switch 48 puertos - San José	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Switch 48 puertos - Ingenio	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Switch 48 puertos - Ingenio	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Switch 48 puertos - Ingenio	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Switch 48 puertos - Ingenio	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Switch 48 puertos - Ingenio	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Access Point - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Access Point - El Rosario	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Access Point - El Rosario	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Access Point - El Rosario	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Access Point - El Rosario	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Access Point - San José	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Access Point - San José	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Access Point - San José	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Access Point - San José	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Access Point - San José	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Access Point - Ingenio	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Access Point - Ingenio	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Access Point - Ingenio	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Access Point - Ingenio	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Access Point - Ingenio	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Routers Inalambricos - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Routers Inalambricos - El Rosario	[I.6]	PR-B	0%	0%	0%	100%	0%

Red	Routers Inalambricos - El Rosario	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Routers Inalambricos - El Rosario	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Routers Inalambricos - El Rosario	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Routers Inalambricos - San José	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Routers Inalambricos - San José	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Routers Inalambricos - San José	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Routers Inalambricos - San José	[E.28]	PR-B	0%	0%	0%	100%	0%
Red	Routers Inalambricos - San José	[A.12]	PR-MB	60%	100%	80%	20%	80%
Red	Routers Inalambricos - Ingenio	[N.*]	PR-MB	0%	0%	0%	100%	0%
Red	Routers Inalambricos - Ingenio	[I.6]	PR-B	0%	0%	0%	100%	0%
Red	Routers Inalambricos - Ingenio	[I.7]	PR-MB	0%	0%	0%	100%	0%
Red	Routers Inalambricos - Ingenio	[E.28]	PR-B	0%	0%	0%	100%	0%
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%
Red	Routers - El Rosario	[A.12]	PR-MB	60%	100%	80%	20%	80%
Hardware	Computadores de Escritorio - San José - Ingenio	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Computadores de Escritorio - San José - Ingenio	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Computadores de Escritorio - San José - Ingenio	[I.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	Computadores de Escritorio - San José - Ingenio	[I.6]	PR-MB	0%	0%	0%	100%	0%
Hardware	Computadores de Escritorio - San José - Ingenio	[E.1]	PR-B	0%	40%	80%	0%	0%

Hardware	Computadores de Escritorio - San José - Ingenio	[E.4]	PR-M	0%	0%	0%	100%	0%
Hardware	Computadores Todo en Uno - Ingenio	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Computadores Todo en Uno - Ingenio	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Computadores Todo en Uno - Ingenio	[I.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	Computadores Todo en Uno - Ingenio	[I.6]	PR-MB	0%	0%	0%	100%	0%
Hardware	Computadores Todo en Uno - Ingenio	[E.1]	PR-B	0%	40%	80%	0%	0%
Hardware	Computadores Todo en Uno - Ingenio	[E.4]	PR-M	0%	0%	0%	100%	0%
Hardware	Portátiles - San José - Ingenio	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Portátiles - San José - Ingenio	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Portátiles - San José - Ingenio	[I.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	Portátiles - San José - Ingenio	[I.6]	PR-MB	0%	0%	0%	100%	0%
Hardware	Portátiles - San José - Ingenio	[E.1]	PR-B	0%	40%	80%	0%	0%
Hardware	Portátiles - San José - Ingenio	[E.4]	PR-M	0%	0%	0%	100%	0%
Hardware	Portátiles - San José - Ingenio	[E.25]	PR-MB	20%	100%	20%	100%	0%
Hardware	Portátiles - San José - Ingenio	[A.25]	PR-B	20%	100%	20%	100%	0%
Hardware	Apple MAC ProBook - San José	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Apple MAC ProBook - San José	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Apple MAC ProBook - San José	[I.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	Apple MAC ProBook - San José	[I.6]	PR-MB	0%	0%	0%	100%	0%
Hardware	Apple MAC ProBook - San José	[E.1]	PR-B	0%	40%	80%	0%	0%
Hardware	Apple MAC ProBook - San José	[E.4]	PR-M	0%	0%	0%	100%	0%
Hardware	Apple MAC ProBook - San José	[E.25]	PR-MB	20%	100%	20%	100%	0%
Hardware	Apple MAC ProBook - San José	[A.25]	PR-B	20%	100%	20%	100%	0%
Hardware	Impresoras - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Impresoras - El Rosario	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Impresoras - El Rosario	[I.2]	PR-MB	0%	0%	0%	100%	0%

Hardware	Impresoras - El Rosario	[I.6]	PR-M	0%	0%	0%	100%	0%
Hardware	Impresoras - El Rosario	[E.1]	PR-M	0%	0%	0%	100%	0%
Hardware	Impresoras - El Ingenio	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Impresoras - El Ingenio	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Impresoras - El Ingenio	[I.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	Impresoras - El Ingenio	[I.6]	PR-M	0%	0%	0%	100%	0%
Hardware	Impresoras - El Ingenio	[E.1]	PR-M	0%	0%	0%	100%	0%
Hardware	Impresoras - San José	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Impresoras - San José	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Impresoras - San José	[I.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	Impresoras - San José	[I.6]	PR-M	0%	0%	0%	100%	0%
Hardware	Impresoras - San José	[E.1]	PR-M	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - El Rosario	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - El Rosario	[I.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - El Rosario	[A.25]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - San José	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - San José	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - San José	[I.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - San José	[A.25]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - Ingenio	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - Ingenio	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - Ingenio	[I.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	Teléfonos IP - Ingenio	[A.25]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - El Rosario	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - El Rosario	[I.2]	PR-B	0%	0%	0%	100%	0%

Hardware	Lectores de tarjetas de proximidad - El Rosario	[I.6]	PR-M	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - El Rosario	[A.23]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - El Rosario	[A.25]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - San José	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - San José	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - San José	[I.2]	PR-B	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - San José	[I.6]	PR-M	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - San José	[A.23]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - San José	[A.25]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.1]	PR-MB	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.2]	PR-B	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.6]	PR-M	0%	0%	0%	100%	0%
Hardware	Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[A.23]	PR-MB	0%	0%	0%	100%	0%

Hardware	Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[A.25]	PR-MB	0%	0%	0%	100%	0%
Hardware	Servidores - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	Servidores - El Rosario	[I.6]	PR-M	0%	0%	0%	100%	0%
Hardware	Servidores - El Rosario	[I.7]	PR-B	0%	0%	0%	100%	0%
Hardware	Servidores - El Rosario	[E.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	Servidores - El Rosario	[E.23]	PR-MB	100%	0%	0%	100%	40%
Hardware	Servidores - El Rosario	[A.6]	PR-MB	0%	0%	0%	100%	40%
Hardware	NAS - El Rosario	[N.*]	PR-MB	0%	0%	0%	100%	0%
Hardware	NAS - El Rosario	[I.6]	PR-M	0%	0%	0%	100%	0%
Hardware	NAS - El Rosario	[I.7]	PR-B	0%	0%	0%	100%	0%
Hardware	NAS - El Rosario	[E.2]	PR-MB	0%	0%	0%	100%	0%
Hardware	NAS - El Rosario	[E.23]	PR-MB	100%	0%	0%	100%	40%
Hardware	NAS - El Rosario	[A.6]	PR-MB	0%	0%	0%	100%	40%
Software	Ofimática - Toda la Institución	[E.20]	PR-MB	0%	100%	50%	100%	0%
Software	Ofimática - Toda la Institución	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Sistema Operativo Cliente - Toda la Institución	[E.20]	PR-MB	0%	100%	50%	100%	0%
Software	Sistema Operativo Cliente - Toda la Institución	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Sistema Operativo Cliente - Toda la Institución	[A.11]	PR-MB	75%	100%	50%	100%	80%
Software	Motor de Base de Datos - Servicios de Gestión Académica.	[E.20]	PR-MB	0%	100%	50%	100%	0%
Software	Motor de Base de Datos - Servicios de Gestión Académica.	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Motor de Base de Datos - Servicios de Gestión Académica.	[A.6]	PR-MB	75%	100%	50%	100%	80%
Software	Motor de Base de Datos - Servicios de Gestión Académica.	[A.11]	PR-MB	75%	100%	50%	100%	80%
Software	Sistema Operativo Servidores - Toda la Institución	[E.20]	PR-MB	0%	100%	50%	100%	0%

Software	Sistema Operativo Servidores - Toda la Institución	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Sistema Operativo Servidores - Toda la Institución	[A.6]	PR-MB	75%	100%	50%	100%	80%
Software	Sistema Operativo Servidores - Toda la Institución	[A.11]	PR-MB	75%	100%	50%	100%	80%
Software	Licencia de Escritorio Remoto - Dispositivo - Servicios de Gestión Académica.	[A.25]	PR-MB	0%	0%	0%	100%	0%
Software	Aplicaciones de Desarrollo - Servicios de Gestión Académica.	[A.25]	PR-MB	0%	0%	0%	100%	0%
Software	Servidor de Terminal Services - Servicios de Gestión Académica.	[E.20]	PR-MB	50%	100%	50%	100%	20%
Software	Servidor de Terminal Services - Servicios de Gestión Académica.	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Servidor de Terminal Services - Servicios de Gestión Académica.	[A.6]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor de Terminal Services - Servicios de Gestión Académica.	[A.11]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor de Terminal Services - Servicios de Gestión Académica.	[E.2]	PR-MB	100%	100%	80%	100%	80%
Software	Servidor Directorio Activo - Toda la Institución	[E.20]	PR-MB	50%	100%	50%	100%	20%
Software	Servidor Directorio Activo - Toda la Institución	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Servidor Directorio Activo - Toda la Institución	[A.6]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor Directorio Activo - Toda la Institución	[A.11]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor Directorio Activo - Toda la Institución	[E.2]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor de Aplicaciones -	[E.20]	PR-MB	50%	100%	50%	100%	20%

	Servicios de Gestión Académica.							
Software	Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Servidor de Aplicaciones - Servicios de Gestión Académica.	[A.6]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor de Aplicaciones - Servicios de Gestión Académica.	[A.11]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.2]	PR-MB	75%	100%	50%	100%	80%
Software	Licencia de Antivirus Clientes - Toda la Institución	[A.25]	PR-MB	0%	0%	0%	100%	40%
Software	Servidor DHCP - Toda la Institución	[E.20]	PR-MB	50%	0%	0%	100%	20%
Software	Servidor DHCP - Toda la Institución	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Servidor DHCP - Toda la Institución	[A.6]	PR-MB	75%	0%	0%	100%	80%
Software	Servidor DHCP - Toda la Institución	[A.11]	PR-MB	75%	0%	0%	100%	80%
Software	Servidor DHCP - Toda la Institución	[E.2]	PR-MB	75%	0%	0%	100%	80%
Software	Servidor Antivirus - Toda la Institución	[E.20]	PR-MB	50%	0%	0%	100%	20%
Software	Servidor Antivirus - Toda la Institución	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Servidor Antivirus - Toda la Institución	[A.6]	PR-MB	75%	0%	0%	100%	80%
Software	Servidor Antivirus - Toda la Institución	[A.11]	PR-MB	75%	0%	0%	100%	80%
Software	Servidor Antivirus - Toda la Institución	[E.2]	PR-MB	75%	0%	0%	100%	80%
Software	Servidor de Backup MV - Toda la Institución	[E.20]	PR-MB	50%	100%	50%	100%	20%
Software	Servidor de Backup MV - Toda la Institución	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Servidor de Backup MV - Toda la Institución	[A.6]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor de Backup MV - Toda la Institución	[A.11]	PR-MB	75%	100%	50%	100%	80%

Software	Servidor de Backup MV - Toda la Institución	[E.2]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.20]	PR-MB	50%	100%	50%	100%	20%
Software	Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.21]	PR-B	0%	0%	0%	100%	40%
Software	Servidor de Backup Archivos - Servicios de Gestión Académica.	[A.6]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor de Backup Archivos - Servicios de Gestión Académica.	[A.11]	PR-MB	75%	100%	50%	100%	80%
Software	Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.2]	PR-MB	75%	100%	50%	100%	80%
Datos	Base de Datos Estudiantes - Servicios de Gestión Académica.	[E.1]	PR-B	0%	100%	100%	10%	80%
Datos	Base de Datos Estudiantes - Servicios de Gestión Académica.	[E.15]	PR-B	0%	20%	100%	80%	80%
Datos	Base de Datos Estudiantes - Servicios de Gestión Académica.	[A.11]	PR-MB	75%	100%	50%	100%	80%
Datos	Base de Datos Docentes - Servicios de Gestión Académica.	[E.1]	PR-B	0%	100%	100%	10%	80%
Datos	Base de Datos Docentes - Servicios de Gestión Académica.	[E.15]	PR-B	0%	20%	100%	80%	80%
Datos	Base de Datos Docentes - Servicios de Gestión Académica.	[A.11]	PR-MB	75%	100%	50%	100%	80%
Datos	Base de Datos Personal Administrativo - Toda la Institución	[E.1]	PR-B	0%	100%	100%	10%	80%
Datos	Base de Datos Personal Administrativo - Toda la Institución	[E.15]	PR-B	0%	20%	100%	80%	80%

Datos	Base de Datos Personal Administrativo - Toda la Institución	[A.11]	PR-MB	75%	100%	50%	100%	80%
Personal	Estudiantes - Toda la Institución	[A.5]	PR-MB	0%	100%	0%	0%	0%
Personal	Estudiantes - Toda la Institución	[E.28]	PR-MB	0%	0%	0%	100%	0%
Personal	Docentes - Toda la Institución	[A.5]	PR-MB	80%	100%	100%	100%	0%
Personal	Docentes - Toda la Institución	[E.28]	PR-MB	0%	0%	0%	100%	0%
Personal	Personal Administrativo - Toda la Institución	[E.28]	PR-MB	0%	0%	0%	100%	0%
Personal	Personal Administrativo - Toda la Institución	[A.28]	PR-MB	0%	0%	0%	100%	0%
Personal	Personal Administrativo - Toda la Institución	[A.30]	PR-MB	0%	50%	0%	0%	50%
Personal	Administrador de Infraestructura - Toda la Institución	[E.28]	PR-MB	0%	0%	0%	100%	0%
Personal	Administrador de Infraestructura - Toda la Institución	[A.28]	PR-MB	0%	0%	0%	100%	0%
Personal	Administrador de Infraestructura - Toda la Institución	[A.30]	PR-MB	0%	50%	0%	0%	50%
Personal	Administrador Base de Datos - Toda la Institución	[E.28]	PR-MB	0%	0%	0%	100%	0%
Personal	Administrador Base de Datos - Toda la Institución	[A.28]	PR-MB	0%	0%	0%	100%	0%
Personal	Administrador Base de Datos - Toda la Institución	[A.30]	PR-MB	0%	50%	0%	0%	50%
Servicios	Correo Electrónico - Google Suite	[I.8]	PR-MB	0%	0%	0%	100%	0%
Servicios	Correo Electrónico - Google Suite	[E.2]	PR-MB	40%	100%	80%	100%	80%
Servicios	Correo Electrónico - Google Suite	[A.24]	PR-MB	0%	0%	0%	100%	0%
Servicios	Herramienta Colaborativa - Google Suite	[I.8]	PR-MB	0%	0%	0%	100%	0%
Servicios	Herramienta Colaborativa - Google Suite	[E.2]	PR-MB	40%	100%	80%	100%	80%
Servicios	Herramienta Colaborativa - Google Suite	[A.24]	PR-MB	0%	0%	0%	100%	0%

Servicios	IaaS - CNT	[I.8]	PR-MB	0%	0%	0%	100%	0%
Servicios	IaaS - CNT	[E.2]	PR-MB	40%	100%	80%	100%	80%
Servicios	IaaS - CNT	[A.24]	PR-MB	0%	0%	0%	100%	0%
Servicios	Sistema Académico - Power Campus - Front End	[I.8]	PR-MB	0%	0%	0%	100%	0%
Servicios	Sistema Académico - Power Campus - Front End	[E.1]	PR-MB	40%	100%	80%	100%	80%
Servicios	Sistema Académico - Power Campus - Front End	[A.24]	PR-MB	0%	0%	0%	100%	0%
Servicios	Sistema Académico - Power Campus - Back End	[I.8]	PR-MB	0%	0%	0%	100%	0%
Servicios	Sistema Académico - Power Campus - Back End	[E.2]	PR-MB	40%	100%	80%	100%	80%
Servicios	Sistema Académico - Power Campus - Back End	[A.24]	PR-MB	0%	0%	0%	100%	0%
Servicios	Sistema Virtual de Aprendizaje - D2L - Front End	[I.8]	PR-MB	0%	0%	0%	100%	0%
Servicios	Sistema Virtual de Aprendizaje - D2L - Front End	[E.1]	PR-MB	40%	100%	80%	20%	80%
Servicios	Sistema Virtual de Aprendizaje - D2L - Front End	[A.24]	PR-MB	0%	0%	0%	100%	0%
Servicios	Sistema Virtual de Aprendizaje - D2L - Back End	[I.8]	PR-MB	0%	0%	0%	100%	0%
Servicios	Sistema Virtual de Aprendizaje - D2L - Back End	[E.2]	PR-MB	40%	100%	80%	100%	80%
Servicios	Sistema Virtual de Aprendizaje - D2L - Back End	[A.24]	PR-MB	0%	0%	0%	100%	0%
Servicios	Usuario Externo -	[E.28]	PR-MB	0%	0%	0%	50%	0%
Servicios	Usuario Interno -	[E.28]	PR-MB	0%	0%	0%	50%	0%

Cuadro 7: Tabla de degradación dimensiones de la seguridad por amenaza y frecuencia

Notemos como en la fila identificadora del activo, anotamos como impacto el máximo de los impactos que pueden provocar las diferentes amenazas.

Una reflexión antes de proseguir: el riesgo no será en general eliminable (por ejemplo, probablemente no podremos aislar nuestra empresa o hacerla inmune a los desastres naturales), pero sí gestionable. Recordemos que habitualmente, el riesgo se gestiona no se elimina.

3.7 Impacto potencial

Una vez realizada la tabla anterior, y dado que conocemos los valores de los diferentes activos, podemos determinar el impacto potencial que puede suponer para la empresa la materialización de las amenazas. Se trata de un dato relevante, ya que permitirá priorizar el plan de acción, y a su vez, evaluar cómo se ve modificado dicho valor una vez se apliquen contramedidas.

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 (Ver Tabla 6) con la degradación en las diferentes dimensiones de seguridad que se ve afectado por una amenaza (Ver Tabla 7).

Teniendo el siguiente resultado:

Activo	Amenaza	Frecuencia	IMPACTO				
			A	C	I	D	T
Data Center - El Rosario	[N.*]	PR-MB				MA	
Data Center - El Rosario	[I.*]	PR-MB				MA	
Data Center - El Rosario	[I.6]	PR-B				MA	
Data Center - El Rosario	[A.11]	PR-MB		MA		MA	MA
Cuarto de Rack - San José	[N.*]	PR-MB				A	
Cuarto de Rack - San José	[I.*]	PR-MB				A	
Cuarto de Rack - San José	[I.6]	PR-B				A	
Cuarto de Rack - Ingenio – Principal	[N.*]	PR-MB				MA	
Cuarto de Rack - Ingenio – Principal	[I.*]	PR-MB				MA	
Cuarto de Rack - Ingenio – Principal	[I.6]	PR-B				MA	
Cuarto de Rack - Ingenio – Biblioteca	[N.*]	PR-MB				MA	
Cuarto de Rack - Ingenio – Biblioteca	[I.*]	PR-MB				MA	
Cuarto de Rack - Ingenio – Biblioteca	[I.6]	PR-B				MA	
Cuarto de Rack - Ingenio – Aulas	[N.*]	PR-MB				MA	
Cuarto de Rack - Ingenio – Aulas	[I.*]	PR-MB				MA	
Cuarto de Rack - Ingenio – Aulas	[I.6]	PR-B				MA	
Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[N.*]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[E.25]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[A.12]	PR-B				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[N.*]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[E.25]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[A.12]	PR-B				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo – Ingenio	[N.*]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo – Ingenio	[E.25]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo – Ingenio	[A.12]	PR-B				A	

Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[N.*]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[E.25]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[A.14]	PR-B	M	M		M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[N.*]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[E.25]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[A.14]	PR-B	M	M		M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red – Ingenio	[N.*]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red – Ingenio	[E.25]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red – Ingenio	[A.14]	PR-B	M	M		M	
Switch Core - El Rosario	[N.*]	PR-MB				MA	
Switch Core - El Rosario	[I.6]	PR-B				MA	
Switch Core - El Rosario	[I.7]	PR-MB				MA	
Switch Core - El Rosario	[E.28]	PR-B				MA	
Switch Core - El Rosario	[A.12]	PR-MB	MA	MA	MA	A	MA
Switch 24 puertos - El Rosario	[N.*]	PR-MB				A	
Switch 24 puertos - El Rosario	[I.6]	PR-B				A	
Switch 24 puertos - El Rosario	[I.7]	PR-MB				A	
Switch 24 puertos - El Rosario	[E.28]	PR-B				A	
Switch 24 puertos - El Rosario	[A.12]	PR-MB	A	A	A	B	A
Switch 24 puertos – Ingenio	[N.*]	PR-MB				A	
Switch 24 puertos – Ingenio	[I.6]	PR-B				A	
Switch 24 puertos – Ingenio	[I.7]	PR-MB				A	
Switch 24 puertos – Ingenio	[E.28]	PR-B				A	
Switch 24 puertos – Ingenio	[A.12]	PR-MB	A	A	A	B	A
Switch 48 puertos - El Rosario – Residencias	[N.*]	PR-MB				A	
Switch 48 puertos - El Rosario – Residencias	[I.6]	PR-B				A	
Switch 48 puertos - El Rosario – Residencias	[I.7]	PR-MB				A	
Switch 48 puertos - El Rosario – Residencias	[E.28]	PR-B				A	
Switch 48 puertos - El Rosario – Residencias	[A.12]	PR-MB	A	A	A	B	A
Switch 48 puertos - San José	[N.*]	PR-MB				A	
Switch 48 puertos - San José	[I.6]	PR-B				A	
Switch 48 puertos - San José	[I.7]	PR-MB				A	
Switch 48 puertos - San José	[E.28]	PR-B				A	
Switch 48 puertos - San José	[A.12]	PR-MB	A	A	A	B	A
Switch 48 puertos – Ingenio	[N.*]	PR-MB				A	
Switch 48 puertos – Ingenio	[I.6]	PR-B				A	
Switch 48 puertos – Ingenio	[I.7]	PR-MB				A	
Switch 48 puertos – Ingenio	[E.28]	PR-B				A	
Switch 48 puertos – Ingenio	[A.12]	PR-MB	A	A	A	B	A

Access Point - El Rosario	[N.*]	PR-MB				M		
Access Point - El Rosario	[I.6]	PR-B				M		
Access Point - El Rosario	[I.7]	PR-MB				M		
Access Point - El Rosario	[E.28]	PR-B				M		
Access Point - El Rosario	[A.12]	PR-MB	M	M	M	MB	M	
Access Point - San José	[N.*]	PR-MB				M		
Access Point - San José	[I.6]	PR-B				M		
Access Point - San José	[I.7]	PR-MB				M		
Access Point - San José	[E.28]	PR-B				M		
Access Point - San José	[A.12]	PR-MB	M	M	M	MB	M	
Access Point – Ingenio	[N.*]	PR-MB				M		
Access Point – Ingenio	[I.6]	PR-B				M		
Access Point – Ingenio	[I.7]	PR-MB				M		
Access Point – Ingenio	[E.28]	PR-B				M		
Access Point – Ingenio	[A.12]	PR-MB	M	M	M	MB	M	
Routers Inalambricos - El Rosario	[N.*]	PR-MB				M		
Routers Inalambricos - El Rosario	[I.6]	PR-B				M		
Routers Inalambricos - El Rosario	[I.7]	PR-MB				M		
Routers Inalambricos - El Rosario	[E.28]	PR-B				M		
Routers Inalambricos - El Rosario	[A.12]	PR-MB	M	M	M	MB	M	
Routers Inalambricos - San José	[N.*]	PR-MB				M		
Routers Inalambricos - San José	[I.6]	PR-B				M		
Routers Inalambricos - San José	[I.7]	PR-MB				M		
Routers Inalambricos - San José	[E.28]	PR-B				M		
Routers Inalambricos - San José	[A.12]	PR-MB	M	M	M	MB	M	
Routers Inalambricos – Ingenio	[N.*]	PR-MB				M		
Routers Inalambricos – Ingenio	[I.6]	PR-B				M		
Routers Inalambricos – Ingenio	[I.7]	PR-MB				M		
Routers Inalambricos – Ingenio	[E.28]	PR-B				M		
Routers Inalambricos – Ingenio	[A.12]	PR-MB	M	M	M	MB	M	
Firewall - El Rosario	[N.*]	PR-MB				MA		
Firewall - El Rosario	[I.6]	PR-B				MA		
Firewall - El Rosario	[I.7]	PR-MB				MA		
Firewall - El Rosario	[A.11]	PR-MB	MA	MA	MA	MA	MA	
Firewall - El Rosario	[A.24]	PR-MB				MA		
Routers - El Rosario	[N.*]	PR-MB				MA		
Routers - El Rosario	[I.6]	PR-B				MA		
Routers - El Rosario	[I.7]	PR-MB				MA		
Routers - El Rosario	[E.28]	PR-B				MA		

Routers - El Rosario	[A.12]	PR-MB	MA	MA	MA	M	MA
Computadores de Escritorio - San José – Ingenio	[N.*]	PR-MB				M	
Computadores de Escritorio - San José – Ingenio	[I.1]	PR-MB				M	
Computadores de Escritorio - San José – Ingenio	[I.2]	PR-MB				M	
Computadores de Escritorio - San José – Ingenio	[I.6]	PR-MB				M	
Computadores de Escritorio - San José – Ingenio	[E.1]	PR-B		B	M		
Computadores de Escritorio - San José – Ingenio	[E.4]	PR-M				M	
Computadores Todo en Uno – Ingenio	[N.*]	PR-MB				B	
Computadores Todo en Uno – Ingenio	[I.1]	PR-MB				B	
Computadores Todo en Uno – Ingenio	[I.2]	PR-MB				B	
Computadores Todo en Uno – Ingenio	[I.6]	PR-MB				B	
Computadores Todo en Uno – Ingenio	[E.1]	PR-B		MB	B		
Computadores Todo en Uno – Ingenio	[E.4]	PR-M				B	
Portátiles - San José – Ingenio	[N.*]	PR-MB				M	
Portátiles - San José – Ingenio	[I.1]	PR-MB				M	
Portátiles - San José – Ingenio	[I.2]	PR-MB				M	
Portátiles - San José – Ingenio	[I.6]	PR-MB				M	
Portátiles - San José – Ingenio	[E.1]	PR-B		B	M		
Portátiles - San José – Ingenio	[E.4]	PR-M				M	
Portátiles - San José – Ingenio	[E.25]	PR-MB	MB	M	MB	M	
Portátiles - San José – Ingenio	[A.25]	PR-B	MB	M	MB	M	
Apple MAC ProBook - San José	[N.*]	PR-MB				B	
Apple MAC ProBook - San José	[I.1]	PR-MB				B	
Apple MAC ProBook - San José	[I.2]	PR-MB				B	
Apple MAC ProBook - San José	[I.6]	PR-MB				B	
Apple MAC ProBook - San José	[E.1]	PR-B		MB	B		
Apple MAC ProBook - San José	[E.4]	PR-M				B	
Apple MAC ProBook - San José	[E.25]	PR-MB	MB	B	MB	B	
Apple MAC ProBook - San José	[A.25]	PR-B	MB	B	MB	B	
Impresoras - El Rosario	[N.*]	PR-MB				A	
Impresoras - El Rosario	[I.1]	PR-MB				A	
Impresoras - El Rosario	[I.2]	PR-MB				A	
Impresoras - El Rosario	[I.6]	PR-M				A	
Impresoras - El Rosario	[E.1]	PR-M				A	
Impresoras - El Ingenio	[N.*]	PR-MB				A	
Impresoras - El Ingenio	[I.1]	PR-MB				A	
Impresoras - El Ingenio	[I.2]	PR-MB				A	
Impresoras - El Ingenio	[I.6]	PR-M				A	
Impresoras - El Ingenio	[E.1]	PR-M				A	
Impresoras - San José	[N.*]	PR-MB				A	

Impresoras - San José	[I.1]	PR-MB				A	
Impresoras - San José	[I.2]	PR-MB				A	
Impresoras - San José	[I.6]	PR-M				A	
Impresoras - San José	[E.1]	PR-M				A	
Teléfonos IP - El Rosario	[N.*]	PR-MB				M	
Teléfonos IP - El Rosario	[I.1]	PR-MB				M	
Teléfonos IP - El Rosario	[I.2]	PR-MB				M	
Teléfonos IP - El Rosario	[A.25]	PR-MB				M	
Teléfonos IP - San José	[N.*]	PR-MB				M	
Teléfonos IP - San José	[I.1]	PR-MB				M	
Teléfonos IP - San José	[I.2]	PR-MB				M	
Teléfonos IP - San José	[A.25]	PR-MB				M	
Teléfonos IP – Ingenio	[N.*]	PR-MB				M	
Teléfonos IP – Ingenio	[I.1]	PR-MB				M	
Teléfonos IP – Ingenio	[I.2]	PR-MB				M	
Teléfonos IP – Ingenio	[A.25]	PR-MB				M	
Lectores de tarjetas de proximidad - El Rosario	[N.*]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Rosario	[I.1]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Rosario	[I.2]	PR-B				MA	
Lectores de tarjetas de proximidad - El Rosario	[I.6]	PR-M				MA	
Lectores de tarjetas de proximidad - El Rosario	[A.23]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Rosario	[A.25]	PR-MB				MA	
Lectores de tarjetas de proximidad - San José	[N.*]	PR-MB				MA	
Lectores de tarjetas de proximidad - San José	[I.1]	PR-MB				MA	
Lectores de tarjetas de proximidad - San José	[I.2]	PR-B				MA	
Lectores de tarjetas de proximidad - San José	[I.6]	PR-M				MA	
Lectores de tarjetas de proximidad - San José	[A.23]	PR-MB				MA	
Lectores de tarjetas de proximidad - San José	[A.25]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[N.*]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.1]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.2]	PR-B				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.6]	PR-M				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[A.23]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[A.25]	PR-MB				MA	
Servidores - El Rosario	[N.*]	PR-MB				MA	
Servidores - El Rosario	[I.6]	PR-M				MA	
Servidores - El Rosario	[I.7]	PR-B				MA	
Servidores - El Rosario	[E.2]	PR-MB				MA	
Servidores - El Rosario	[E.23]	PR-MB	MA			MA	A

Servidores - El Rosario	[A.6]	PR-MB				MA	A
NAS - El Rosario	[N.*]	PR-MB				M	
NAS - El Rosario	[I.6]	PR-M				M	
NAS - El Rosario	[I.7]	PR-B				M	
NAS - El Rosario	[E.2]	PR-MB				M	
NAS - El Rosario	[E.23]	PR-MB	M			M	B
NAS - El Rosario	[A.6]	PR-MB				M	B
Ofimática - Toda la Institución	[E.20]	PR-MB		M	M	M	
Ofimática - Toda la Institución	[E.21]	PR-B				M	B
Sistema Operativo Cliente - Toda la Institución	[E.20]	PR-MB		M	M	M	
Sistema Operativo Cliente - Toda la Institución	[E.21]	PR-B				M	B
Sistema Operativo Cliente - Toda la Institución	[A.11]	PR-MB	M	M	M	M	M
Motor de Base de Datos - Servicios de Gestión Académica.	[E.20]	PR-MB		MA	MA	MA	
Motor de Base de Datos - Servicios de Gestión Académica.	[E.21]	PR-B				MA	MA
Motor de Base de Datos - Servicios de Gestión Académica.	[A.6]	PR-MB	MA	MA	MA	MA	MA
Motor de Base de Datos - Servicios de Gestión Académica.	[A.11]	PR-MB	MA	MA	MA	MA	MA
Sistema Operativo Servidores - Toda la Institución	[E.20]	PR-MB		A	A	A	
Sistema Operativo Servidores - Toda la Institución	[E.21]	PR-B				A	M
Sistema Operativo Servidores - Toda la Institución	[A.6]	PR-MB	A	A	A	A	A
Sistema Operativo Servidores - Toda la Institución	[A.11]	PR-MB	A	A	A	A	A
Licencia de Escritorio Remoto - Dispositivo - Servicios de Gestión Académica.	[A.25]	PR-MB				A	
Aplicaciones de Desarrollo - Servicios de Gestión Académica.	[A.25]	PR-MB				A	
Servidor de Terminal Services - Servicios de Gestión Académica.	[E.20]	PR-MB	A	A	A	A	B
Servidor de Terminal Services - Servicios de Gestión Académica.	[E.21]	PR-B				A	M
Servidor de Terminal Services - Servicios de Gestión Académica.	[A.6]	PR-MB	A	A	A	A	A
Servidor de Terminal Services - Servicios de Gestión Académica.	[A.11]	PR-MB	A	A	A	A	A
Servidor de Terminal Services - Servicios de Gestión Académica.	[E.2]	PR-MB	A	A	A	A	A
Servidor Directorio Activo - Toda la Institución	[E.20]	PR-MB	MA	MA	MA	MA	A
Servidor Directorio Activo - Toda la Institución	[E.21]	PR-B				MA	MA
Servidor Directorio Activo - Toda la Institución	[A.6]	PR-MB	MA	MA	MA	MA	MA
Servidor Directorio Activo - Toda la Institución	[A.11]	PR-MB	MA	MA	MA	MA	MA
Servidor Directorio Activo - Toda la Institución	[E.2]	PR-MB	MA	MA	MA	MA	MA
Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.20]	PR-MB	MA	MA	MA	MA	M
Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.21]	PR-B				MA	A
Servidor de Aplicaciones - Servicios de Gestión Académica.	[A.6]	PR-MB	MA	MA	MA	MA	MA
Servidor de Aplicaciones - Servicios de Gestión Académica.	[A.11]	PR-MB	MA	MA	MA	MA	MA
Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.2]	PR-MB	MA	MA	MA	MA	MA
Licencia de Antivirus Clientes - Toda la Institución	[A.25]	PR-MB				A	B
Servidor DHCP - Toda la Institución	[E.20]	PR-MB	MA			MA	M

Servidor DHCP - Toda la Institución	[E.21]	PR-B				MA	A
Servidor DHCP - Toda la Institución	[A.6]	PR-MB	MA			MA	MA
Servidor DHCP - Toda la Institución	[A.11]	PR-MB	MA			MA	MA
Servidor DHCP - Toda la Institución	[E.2]	PR-MB	MA			MA	MA
Servidor Antivirus - Toda la Institución	[E.20]	PR-MB	A			A	B
Servidor Antivirus - Toda la Institución	[E.21]	PR-B				A	M
Servidor Antivirus - Toda la Institución	[A.6]	PR-MB	A			A	A
Servidor Antivirus - Toda la Institución	[A.11]	PR-MB	A			A	A
Servidor Antivirus - Toda la Institución	[E.2]	PR-MB	A			A	A
Servidor de Backup MV - Toda la Institución	[E.20]	PR-MB	MA	MA	MA	MA	M
Servidor de Backup MV - Toda la Institución	[E.21]	PR-B				MA	A
Servidor de Backup MV - Toda la Institución	[A.6]	PR-MB	MA	MA	MA	MA	MA
Servidor de Backup MV - Toda la Institución	[A.11]	PR-MB	MA	MA	MA	MA	MA
Servidor de Backup MV - Toda la Institución	[E.2]	PR-MB	MA	MA	MA	MA	MA
Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.20]	PR-MB	MA	MA	MA	MA	A
Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.21]	PR-B				MA	MA
Servidor de Backup Archivos - Servicios de Gestión Académica.	[A.6]	PR-MB	MA	MA	MA	MA	MA
Servidor de Backup Archivos - Servicios de Gestión Académica.	[A.11]	PR-MB	MA	MA	MA	MA	MA
Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.2]	PR-MB	MA	MA	MA	MA	MA
Base de Datos Estudiantes - Servicios de Gestión Académica.	[E.1]	PR-B		MA	MA	MA	MA
Base de Datos Estudiantes - Servicios de Gestión Académica.	[E.15]	PR-B		A	MA	MA	MA
Base de Datos Estudiantes - Servicios de Gestión Académica.	[A.11]	PR-MB	MA	MA	MA	MA	MA
Base de Datos Docentes - Servicios de Gestión Académica.	[E.1]	PR-B		MA	MA	MA	MA
Base de Datos Docentes - Servicios de Gestión Académica.	[E.15]	PR-B		A	MA	MA	MA
Base de Datos Docentes - Servicios de Gestión Académica.	[A.11]	PR-MB	MA	MA	MA	MA	MA
Base de Datos Personal Administrativo - Toda la Institución	[E.1]	PR-B		MA	MA	MA	MA
Base de Datos Personal Administrativo - Toda la Institución	[E.15]	PR-B		A	MA	MA	MA
Base de Datos Personal Administrativo - Toda la Institución	[A.11]	PR-MB	MA	MA	MA	MA	MA
Estudiantes - Toda la Institución	[A.5]	PR-MB		MA			
Estudiantes - Toda la Institución	[E.28]	PR-MB				MA	
Docentes - Toda la Institución	[A.5]	PR-MB	MA	MA	MA	MA	
Docentes - Toda la Institución	[E.28]	PR-MB				MA	
Personal Administrativo - Toda la Institución	[E.28]	PR-MB				A	
Personal Administrativo - Toda la Institución	[A.28]	PR-MB				A	
Personal Administrativo - Toda la Institución	[A.30]	PR-MB		A			A
Administrador de Infraestructura - Toda la Institución	[E.28]	PR-MB				MA	
Administrador de Infraestructura - Toda la Institución	[A.28]	PR-MB				MA	
Administrador de Infraestructura - Toda la Institución	[A.30]	PR-MB		MA			MA
Administrador Base de Datos - Toda la Institución	[E.28]	PR-MB				MA	

Administrador Base de Datos - Toda la Institución	[A.28]	PR-MB				MA	
Administrador Base de Datos - Toda la Institución	[A.30]	PR-MB		MA			MA
Correo Electrónico - Google Suite	[I.8]	PR-MB				A	
Correo Electrónico - Google Suite	[E.2]	PR-MB	M	A	A	A	A
Correo Electrónico - Google Suite	[A.24]	PR-MB				A	
Herramienta Colaborativa - Google Suite	[I.8]	PR-MB				M	
Herramienta Colaborativa - Google Suite	[E.2]	PR-MB	B	M	M	M	M
Herramienta Colaborativa - Google Suite	[A.24]	PR-MB				M	
IaaS – CNT	[I.8]	PR-MB				MA	
IaaS – CNT	[E.2]	PR-MB	MA	MA	MA	MA	MA
IaaS – CNT	[A.24]	PR-MB				MA	
Sistema Académico - Power Campus - Front End	[I.8]	PR-MB				MA	
Sistema Académico - Power Campus - Front End	[E.1]	PR-MB	MA	MA	MA	MA	MA
Sistema Académico - Power Campus - Front End	[A.24]	PR-MB				MA	
Sistema Académico - Power Campus - Back End	[I.8]	PR-MB				MA	
Sistema Académico - Power Campus - Back End	[E.2]	PR-MB	MA	MA	MA	MA	MA
Sistema Académico - Power Campus - Back End	[A.24]	PR-MB				MA	
Sistema Virtual de Aprendizaje - D2L -Front End	[I.8]	PR-MB				MA	
Sistema Virtual de Aprendizaje - D2L -Front End	[E.1]	PR-MB	MA	MA	MA	A	MA
Sistema Virtual de Aprendizaje - D2L -Front End	[A.24]	PR-MB				MA	
Sistema Virtual de Aprendizaje - D2L - Back End	[I.8]	PR-MB				MA	
Sistema Virtual de Aprendizaje - D2L - Back End	[E.2]	PR-MB	MA	MA	MA	MA	MA
Sistema Virtual de Aprendizaje - D2L - Back End	[A.24]	PR-MB				MA	
Usuario Externo -	[E.28]	PR-MB				MA	
Usuario Interno -	[E.28]	PR-MB				MA	

Cuadro 25: Tabla de Valoración del Impacto Potencial

3.8 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.

Este nivel de riesgo aceptable tiene que estar aprobado por Dirección, y se tienen que definir los criterios para establecer dicho nivel (Ver ANEXO X).

El objetivo de este paso es identificar los controles que se tiene implementados o planeados implementar, para minimizar o eliminar la probabilidad que una amenaza se concrete.

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 del 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.

Por otra parte, una vez establecido el control, se reducirá el riesgo, pero este seguirá existiendo (lo deseable es conseguir reducirlo para que esté por debajo del nivel aceptable), a este riesgo que seguirá existiendo después de aplicar los controles de seguridad, se denomina riesgo residual.

Para el cálculo del riesgo residual se procederá con cálculo del impacto residual para lo cual se deberá generar nuevamente la tabla 7, pero considerando el porcentaje de eficiencia que tiene la/las salvaguarda(s) (contramedidas) sobre la degradación de las dimensiones de seguridad por cada amenaza detectada, después se procederá con el cálculo de la tabla 8 obteniendo de esta manera el riesgo residual.

3.9 Resultados

Una vez realizadas las tareas contempladas en esta fase, disponemos de los 71 activos analizados, los activos que se encuentran en estado de riesgo potencial Alto y Muy Alto son 46:

1. Administrador Base de Datos - Toda la Institución
2. Administrador de Infraestructura - Toda la Institución
3. Base de Datos Docentes - Servicios de Gestión Académica.
4. Base de Datos Estudiantes - Servicios de Gestión Académica.
5. Base de Datos Personal Administrativo - Toda la Institución
6. Cuarto de Rack - Ingenio - Aulas
7. Cuarto de Rack - Ingenio - Biblioteca
8. Cuarto de Rack - Ingenio - Principal
9. Cuarto de Rack - San José
10. Data Center - El Rosario

11. Docentes - Toda la Institución
12. Estudiantes - Toda la Institución
13. Firewall - El Rosario
14. IaaS - CNT
15. Impresoras - El Ingenio
16. Impresoras - El Rosario
17. Impresoras - San José
18. Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)
19. Lectores de tarjetas de proximidad - El Rosario
20. Lectores de tarjetas de proximidad - San José
21. Motor de Base de Datos - Servicios de Gestión Académica.
22. Puntos de Red – Cableado Estructurado – Puestos de Trabajo - Ingenio
23. Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José
24. Puntos de Red – Cableado Estructurado – Servidores - El Rosario
25. Routers - El Rosario
26. Servidor Antivirus - Toda la Institución
27. Servidor de Aplicaciones - Servicios de Gestión Académica.
28. Servidor de Backup Archivos - Servicios de Gestión Académica.
29. Servidor de Backup MV - Toda la Institución
30. Servidor de Terminal Services - Servicios de Gestión Académica.
31. Servidor DHCP - Toda la Institución
32. Servidor Directorio Activo - Toda la Institución
33. Servidores - El Rosario
34. Sistema Académico - Power Campus - Back End
35. Sistema Académico - Power Campus - Front End
36. Sistema Operativo Servidores - Toda la Institución
37. Sistema Virtual de Aprendizaje - D2L - Back End
38. Sistema Virtual de Aprendizaje - D2L -Front End
39. Switch 24 puertos - El Rosario
40. Switch 24 puertos - Ingenio
41. Switch 48 puertos - El Rosario - Residencias
42. Switch 48 puertos - Ingenio
43. Switch 48 puertos - San José
44. Switch Core - El Rosario
45. Usuario Externo -
46. Usuario Interno -

Las amenazas principales que podrían materializarse tienen un grado de riesgo potencial Alto y Muy Alto son:

[A.11] Ataques intencionados - Acceso no autorizado

[A.12] Ataques intencionados - Análisis de tráfico

[A.23] Ataques intencionados - Manipulación de los equipos

[A.24] Ataques intencionados - Denegación de servicio

[A.25] Ataques intencionados - Robo

[A.28] Ataques intencionados - Indisponibilidad del personal

[A.5] Ataques intencionados - Suplantación de la identidad del usuario

[A.6] Ataques intencionados - Abuso de privilegios de acceso

[E.1] Errores y fallos no intencionados - Errores de los usuarios

[E.15] Errores y fallos no intencionados - Alteración accidental de la información

[E.2] Errores y fallos no intencionados - Errores del administrador

[E.20] Errores y fallos no intencionados - Vulnerabilidades de los programas (software)

[E.21] Errores y fallos no intencionados - Errores de mantenimiento / actualización de programas (software)

[E.23] Errores y fallos no intencionados - Errores de mantenimiento / actualización de equipos (hardware)

[E.28] Errores y fallos no intencionados - Indisponibilidad del personal

[I.*] De origen industrial - Desastres industriales

[I.1] De origen industrial - Fuego

[I.2] De origen industrial - Daños por agua

[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

[N.*] Desastres naturales - Desastres naturales

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 -

Cuadro 9: 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%.

4 Propuestas de Proyectos

4.1 Introducción

Llegados a este punto, conocemos el nivel de riesgo actual en la Organización, por lo que es el momento de plantear proyectos que mejoren el estado de la seguridad.

4.2 Propuestas

La descripción de las mejoras propuestas (proyectos) deberá ayudar a mitigar el riesgo actual a la organización y evolucionar el cumplimiento ISO hasta un nivel adecuado. Dichos proyectos deben derivarse de los resultados obtenidos en el capítulo 3 “Análisis de Riesgo”, priorizando la implementación de los que aporten mejoras en la seguridad en el menor plazo posible y analizando el impacto económico que tendría su ejecución.

Los proyectos planteados serán resultantes de agrupar un conjunto de recomendaciones identificadas en la fase de análisis de riesgos para facilitar su ejecución. Se incidirá no sólo en la mejora en relación con la gestión de la seguridad, sino también en posibles beneficios colaterales como puede ser la optimización de recursos, mejora en la gestión de procesos y tecnologías presentes en la organización analizada.

Los proyectos deben cuantificarse económicamente y planificarse en el tiempo, estableciendo plazos de consecución de sus objetivos (en general, corto, medio y largo plazo). Adicionalmente, deben incluirse en la planificación puntos de control que permitan considerar realmente el Plan de Implementación del SGSI como un proceso de mejora continua.

Es importante remarcar que los proyectos no deben limitarse al ámbito de la tecnología, sino que pueden (habitualmente, deben) afectar a los diferentes ámbitos (p.e. recursos humanos, organización), los proyectos que se aborden en estos aspectos deben también plantearse.

Se han definido 11 proyectos que a ser implementados a corto, mediano y largo plazo:

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	

Cuadro 10: Proyectos propuestos

A continuación, se describe brevemente los proyectos planteados para minimizar el riesgo:

Código del proyecto: PRJ-001

Nombre del proyecto: Implantación de políticas de seguridad de la información.

Dominios afectados: Políticas de seguridad; aspectos organizativos de la seguridad de la información; seguridad ligada a los recursos humanos; gestión de activos; control de acceso; cifrado; seguridad física y ambiental; seguridad en la operativa; y cumplimiento.

Objetivo: Crear e implantar un conjunto de normas y directrices que conformen la política de seguridad de la información que norme el comportamiento de la organización como un todo, para el cumplimiento del Sistema de Gestión de la Seguridad de la Información (SGSI).

Descripción: Como primera fase del plan, es necesario acordar, a nivel de Dirección de la organización, la política que gobierna la seguridad de la información de la misma, asignando responsabilidades, definiendo procesos y adecuando todo lo relacionado con la seguridad para el correcto cumplimiento de la normativa referente a la seguridad de la información.

Responsable: Rectorado, Cancillería, Coordinación de Planificación, Responsable de sistemas y Tecnología de la Información (Comité de Seguridad de la Información).

Duración: Ha de empezar justo después de finalizar el análisis inicial del estado de madurez de la seguridad, redactando y aprobando documentos que forman parte de la política para solventar o mitigar problemas graves. Se planea finalizar en 4 meses después de la aprobación de la primera versión de la política de seguridad.

Costes: Porcentaje equivalente al 10% del sueldo (por 4 meses) de los integrantes de Dirección (2 personas) más el porcentaje equivalente del 60% del sueldo del responsable de sistemas y TI (por 4 meses). Aproximadamente 7.400 USD en total.

Riesgo a mitigar:

[A.11] Ataques intencionados - Acceso no autorizado,

[A.12] Ataques intencionados - Análisis de tráfico,

[A.23] Ataques intencionados - Manipulación de los equipos,

[A.24] Ataques intencionados - Denegación de servicio,

[A.25] Ataques intencionados - Robo,

[A.28] Ataques intencionados - Indisponibilidad del personal,

[A.5] Ataques intencionados - Suplantación de la identidad del usuario,

[A.6] Ataques intencionados - Abuso de privilegios de acceso,

[E.1] Errores y fallos no intencionados - Errores de los usuarios,

[E.15] Errores y fallos no intencionados - Alteración accidental de la información,

[E.2] Errores y fallos no intencionados - Errores del administrador,

[E.28] Errores y fallos no intencionados - Indisponibilidad del personal

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

Código del proyecto: PRJ-002

Nombre del proyecto: Instalación de un sistema de respaldos y recuperación.

Dominios afectados: Control de acceso, seguridad en la operativa y aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Objetivo: Implementar un sistema centralizado de gestión de tareas de creación, recuperación y almacenamiento de copias de seguridad, tanto de servidores, como de carpetas compartidas y de aplicaciones de negocio como son:

- Sistema Académico - Power Campus - Back End
- Sistema Académico - Power Campus - Front End
- Sistema Virtual de Aprendizaje - D2L - Back End
- Sistema Virtual de Aprendizaje - D2L -Front End

Descripción: Además de la implantación de la política de seguridad, uno de los puntos más críticos para la organización es asegurar la continuidad de negocio y evitar pérdidas de datos. Como se ha comentado, la Universidad maneja información de carácter personal de estudiantes, docentes y personal administrativo, la misma que tiene de carácter confidencial.

Responsable: Responsable de sistemas y tecnologías de la información.

Duración: Ha de empezar justo después de finalizar el análisis inicial del estado de madurez de la seguridad, redactando y aprobando documentos que forman parte de la política para solventar o mitigar problemas graves. Se planea finalizar en 4 meses después de la aprobación de la primera versión de la política de seguridad.

Costes:

- NAS de almacenamiento con 4TB: 700 USD

- Servidor para alojar software de respaldos y recuperación: 2000 USD

- Dedicación del 50% del sueldo de un técnico de sistemas durante 1 mes. Aproximadamente 800 USD.

Riesgo a mitigar:

[A.23] Ataques intencionados - Manipulación de los equipos

[A.24] Ataques intencionados - Denegación de servicio

[A.25] Ataques intencionados - Robo

[E.1] Errores y fallos no intencionados - Errores de los usuarios

[E.15] Errores y fallos no intencionados - Alteración accidental de la información

[E.2] Errores y fallos no intencionados - Errores del administrador

[E.20] Errores y fallos no intencionados - Vulnerabilidades de los programas (software)

[E.21] Errores y fallos no intencionados - Errores de mantenimiento / actualización de programas (software)

[E.23] Errores y fallos no intencionados - Errores de mantenimiento / actualización de equipos (hardware)

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

Código del proyecto: PRJ-003

Nombre del proyecto: Migración de dispositivos de seguridad de red (firewall/IDS/IPS).

Dominios afectados: control de accesos; cifrado; seguridad física y ambiental; seguridad en la operativa; seguridad en las telecomunicaciones; adquisición, desarrollo y mantenimiento de los sistemas de información; y aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Objetivo: Migrar firewall actual debido a que no ofrece las funcionalidades de seguridad y prestaciones necesarias para dar servicio a toda la institución.

Descripción: Se plantea realizar un cambio de firewall y añadir IDS/IPS por uno con mejores prestaciones para asegurar el correcto servicio de TIC. El cambio requiere asignar un equipo de altas prestaciones y poner en alta disponibilidad, gestión de políticas de firewall, creación de túneles VPN, gestión de puntos de acceso Wifi, DMZ, redes externas.

Responsable: Responsable de sistemas y tecnologías de la información.

Duración: Ha de empezar con la solicitud y análisis de propuestas económicas puede empezar mientras se realiza la implantación del Plan. Se planifica para que la implantación dure 1 mes.

Costes:

- Dispositivo de seguridad nuevo: 7.000 USD

- Servicio de Mantenimiento: 2.000 USD

- Porcentaje equivalente al 10% del sueldo del responsable de sistemas y TI (por 1 mes) y el 20% del tiempo de un técnico de sistemas durante 1 mes. Aproximadamente 600 USD.

Riesgo a mitigar:

[A.11] Ataques intencionados - Acceso no autorizado

[A.12] Ataques intencionados - Análisis de tráfico

[A.24] Ataques intencionados - Denegación de servicio

[A.25] Ataques intencionados - Robo

[A.5] Ataques intencionados - Suplantación de la identidad del usuario

[A.6] Ataques intencionados - Abuso de privilegios de acceso

[E.20] Errores y fallos no intencionados - Vulnerabilidades de los programas (software)

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

Código del proyecto: PRJ-004

Nombre del proyecto: Repotenciar Data Center.

Dominios afectados: cifrado, seguridad en la operativa, seguridad en las telecomunicaciones, y aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Objetivo: Poner en alta disponibilidad el Data Center cumpliendo estándares internacionales.

Descripción: Se plantea implementar un data center el mismo que debe cumplir con las norma ANSI –TIA 942 y certificar con Tier 1, esto quiere decir que exista redundancia en energía eléctrica y refrigeración del data center.

Responsable: Responsable de sistemas y tecnologías de la información.

Duración: Debe empezar durante la fase de migración de dispositivos de seguridad de la red. Se plantea dure 1 mes.

Costes:

- Bien:

SISTEMA DE DETECCION Y EXTINCION DE INCENDIOS 9504 USD

SISTEMA DE MONITOREO Y ALARMAS 4062 USD

ENERGÍA REGULADA UPS 4628 USD

ATS - AUTOMATIC TRANSFER SWITCH 1229 USD

EXTENSIONES ELÉCTRICAS RACKS 208 USD

AIRE ACONDICIONADO DE PRECISION 16174 USD

- Servicio: Soporte de mantenimiento anual 2000 USD

- Implantación: el 10% del sueldo del responsable de sistemas por 1 mes más el 40% del sueldo de un técnico de sistemas por 2 meses. Aproximadamente 1800 USD

Riesgo a mitigar:

[E.2] Errores y fallos no intencionados - Errores del administrador

[E.23] Errores y fallos no intencionados - Errores de mantenimiento / actualización de equipos (hardware)

[E.28] Errores y fallos no intencionados - Indisponibilidad del personal

[I.*] De origen industrial - Desastres industriales

[I.1] De origen industrial - Fuego

[I.2] De origen industrial - Daños por agua

[I.6] De origen industrial - Corte del suministro eléctrico

[I.7] De origen industrial - Condiciones inadecuadas de temperatura o humedad

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

Código del proyecto: PRJ-005

Nombre del proyecto: Plan de Formación y Concientización

Dominios afectados: Seguridad Ligada a los Recursos Humanos

Objetivo: Actualizar e implementar el plan de formación del personal en materia de seguridad de la información

Descripción: Se actualiza el plan de formación y capacitación en materia de seguridad de la información.

Este programa de formación está dirigido a todo el personal de la institución (interno y externo) así como los contratistas.

en función a los temas, las disponibilidades y necesidades de formación identificadas para los distintos miembros del personal.

En este plan de formación están incluidos personal, interno y externo.

Este programa de formación es obligatorio para todo el personal (interno y externo) y debe estar finalizado el año en curso.

Responsable: Responsable de sistemas y tecnologías de la información, Director de Talento Humano.

Duración: Debe empezar después de la Implantación de políticas de seguridad de la información. Se plantea dure 2 mes para lo cual se deberá crear grupos para estudiantes, docentes y personal administrativo.

Costes:

- Bien:

Sistema E-Learning1000 USD

- Servicio: Soporte de mantenimiento anual 500 USD

- Implantación: el 10% del sueldo del responsable de sistemas por 1 mes más el 40% del sueldo de un técnico de sistemas por 2 meses. Aproximadamente 1800 USD

Riesgo a mitigar:

[E.1] Errores y fallos no intencionados - Errores de los usuarios

[E.15] Errores y fallos no intencionados - Alteración accidental de la información

[E.2] Errores y fallos no intencionados - Errores del administrador

[E.20] Errores y fallos no intencionados - Vulnerabilidades de los programas (software)

[E.21] Errores y fallos no intencionados - Errores de mantenimiento / actualización de programas (software)

[E.23] Errores y fallos no intencionados - Errores de mantenimiento / actualización de equipos (hardware)

[E.28] Errores y fallos no intencionados - Indisponibilidad del personal

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

Código del proyecto: PRJ-006

Nombre del proyecto: Políticas de control de acceso a la red y servicios de red.

Dominios afectados: Control de Accesos

Objetivo: Revisar y Actualizar el documento de políticas de control de acceso a la información.

Definir y actualizar las reglas de acceso a los diferentes activos y servicios en red.

Descripción: Este proyecto busca actualizar las políticas con referencia al control de acceso a la información dentro de la institución, así como del uso de las redes y los servicios en red.

Estas políticas de control de acceso están basadas en los requerimientos del negocio y la seguridad de la información requerida.

El documento de la política deberá establecer las reglas de acceso, físicas y lógicas, para cada tipo de usuario.

Definir los procedimientos que se van a utilizar para conceder privilegios de acceso y designar los responsables de los mismos.

Este proyecto busca disminuir el número de accesos y conexiones no autorizadas e inseguras a la información, la red y/o servicios de red.

Responsable: Responsable de sistemas y tecnologías de la información

Duración: Debe empezar durante la fase de formación y concientización; y Migración de dispositivos de seguridad de red (firewall/IDS/IPS). Se plantea dure 1 mes.

Costes:

- Implantación: el 10% del sueldo del responsable de sistemas por 1 mes más el 40% del sueldo de un técnico de sistemas por 1 mes. Aproximadamente 800 USD

Riesgo a mitigar:

[E.1] Errores y fallos no intencionados - Errores de los usuarios

[E.15] Errores y fallos no intencionados - Alteración accidental de la información

[E.2] Errores y fallos no intencionados - Errores del administrador

[E.20] Errores y fallos no intencionados - Vulnerabilidades de los programas (software)

[E.21] Errores y fallos no intencionados - Errores de mantenimiento / actualización de programas (software)

[E.23] Errores y fallos no intencionados - Errores de mantenimiento / actualización de equipos (hardware)

[E.28] Errores y fallos no intencionados - Indisponibilidad del personal

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

Código del proyecto: PRJ-007

Nombre del proyecto: Control de acceso al sistema y aplicaciones.

Dominios afectados: Control de Accesos

Objetivo: Evitar los accesos no autorizados a los sistemas y aplicaciones.

Descripción: Este proyecto busca evitar los accesos no autorizados a los sistemas y las aplicaciones.

Para ello se busca:

- Restringir el acceso a la información y a las funciones de las aplicaciones de acuerdo a las políticas de acceso definidas.
- Definir un procedimiento de control de inicio de sesión seguro cuando así se lo requiera.
- Definir un sistema de gestión de contraseñas interactivos y que generen contraseñas de calidad.
- Restringir y controlar los programas utilitarios que anulan el sistema y los controles de aplicación.
- Restringir el acceso a los códigos fuente de los programas**.**

Responsable: Responsable de sistemas y tecnologías de la información

Duración: Debe empezar durante las Políticas de control de acceso. Se plantea dure 2 mes.

Costes:

- Implantación: el 10% del sueldo del responsable de sistemas por 1 mes más el 40% del sueldo de un técnico de sistemas por 2 meses. Aproximadamente 1800 USD

Riesgo a mitigar:

[E.1] Errores y fallos no intencionados - Errores de los usuarios

[E.15] Errores y fallos no intencionados - Alteración accidental de la información

[E.2] Errores y fallos no intencionados - Errores del administrador

[E.20] Errores y fallos no intencionados - Vulnerabilidades de los programas (software)

[E.21] Errores y fallos no intencionados - Errores de mantenimiento / actualización de programas (software)

[E.23] Errores y fallos no intencionados - Errores de mantenimiento / actualización de equipos (hardware)

[E.28] Errores y fallos no intencionados - Indisponibilidad del personal

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

Código del proyecto: PRJ-008

Nombre del proyecto: Control de acceso al sistema y aplicaciones.

Dominios afectados: Control de Accesos, Seguridad en la Operatividad.

Objetivo: Definir procesos y procedimientos formales para asegurar el acceso solo a los usuarios autorizados a los sistemas y servicios.

Descripción: Este proyecto busca definir procesos y procedimientos formales para.

- Altas y bajas de usuarios
- Asignación de acceso de usuarios
- Gestión de los privilegios
- Gestión de las contraseñas de los usuarios
- Revisión de los derechos de acceso

Responsable: Responsable de sistemas y tecnologías de la información

Duración: Debe empezar durante la fase de formación y concientización; y Políticas de control de acceso a la red y servicios de red. Se plantea dure 2 mes.

Costes:

- Implantación: el 10% del sueldo del responsable de sistemas por 1 mes más el 40% del sueldo de un técnico de sistemas por 2 meses. Aproximadamente 1800 USD

Riesgo a mitigar:

[A.11] Ataques intencionados - Acceso no autorizado

[A.12] Ataques intencionados - Análisis de tráfico

[A.23] Ataques intencionados - Manipulación de los equipos

[A.25] Ataques intencionados - Robo

[A.6] Ataques intencionados - Abuso de privilegios de acceso

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

Código del proyecto: PRJ-009

Nombre del proyecto: Mejora en la gestión de Recursos Humanos.

Dominios afectados: Seguridad Ligada a los Recursos Humanos, Seguridad en las Telecomunicaciones, y Cumplimiento

Objetivo: Modificar y completar los procesos y procedimientos de la Gestión de TH.

Descripción: Modificar y completar los procesos asociados a la seguridad ligada a los recursos humanos.

El objetivo es que todos los empleados y proveedores de servicios apliquen la seguridad de la información, se responsabilicen del manejo de la información y estén sometidos a procesos disciplinarios en caso de infracciones.

Se actualizarán los procesos en materia de seguridad para las contrataciones y los retiros del personal.

Responsable: Director de Talento Humano

Duración: Debe empezar a mitad de la fase. Se plantea dure 6 mes.

Costes:

- Implantación: el 10% del sueldo del Director de Talento Humano por 6 meses más el 20% del sueldo de un técnico de Talento Humano por 6 meses. Aproximadamente 2300 USD

Riesgo a mitigar:

[A.11] Ataques intencionados - Acceso no autorizado

[A.6] Ataques intencionados - Abuso de privilegios de acceso

[E.1] Errores y fallos no intencionados - Errores de los usuarios

[E.2] Errores y fallos no intencionados - Errores del administrador

[E.28] Errores y fallos no intencionados - Indisponibilidad del personal

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

Código del proyecto: PRJ-010

Nombre del proyecto: Clasificación de la Información.

Dominios afectados: Gestión de Activos, y Control de Accesos.

Objetivo: Clasificar y etiquetar la información.

Asegurar que se aplique un nivel de protección adecuado a la información.

Descripción: Revisar la clasificación de la información en términos de los requisitos legales, valores críticos y sensibilidad para su divulgación y/o modificación.

Se revisan, modifican y definen nuevos procedimientos para el etiquetado de la información.

Verificar que el esquema de clasificación de la información permite comunicar las prioridades, necesidades de aplicación de medidas especiales de tratamiento y de definir un conjunto adecuado de niveles de protección

Responsable: Responsable de sistemas y tecnologías de la información, Responsable de Seguridad de la Información y propietarios de información.

Duración: Debe empezar durante la fase de formación y concientización; y Políticas de control de acceso a la red y servicios de red. Se plantea dure 2 mes.

Costes:

- Implantación: el 10% del sueldo del responsable de sistemas por 6 mes, más el 40% del sueldo del responsable de seguridad por 6 meses, más el 40% del sueldo de cada responsable de la información por 6 meses. Aproximadamente 6800 USD

Riesgo a mitigar:

[A.11] Ataques intencionados - Acceso no autorizado

[A.25] Ataques intencionados – Robo

[A.6] Ataques intencionados - Abuso de privilegios de acceso

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

Código del proyecto: PRJ-011

Nombre del proyecto: Implementar un CSIRT.

Dominios afectados: gestión de incidentes en la seguridad de la información.

Objetivo: construir y proponer una normativa de seguridad aplicable al entorno local, la implementación del equipo permitirá compartir la experiencia y resultados obtenidos con otras universidades a través de organismos como CEDIA con el objetivo de proponer la creación de una red nacional de CSIRTs.

Descripción: Crear e Implementar un CSIRT Académico para la institución, tiene como objetivo fundamental, el construir y proponer una normativa de seguridad aplicable al entorno local, la implementación del equipo permitirá compartir la experiencia y resultados obtenidos con otras universidades a través de organismos como CEDIA con el objetivo de proponer la creación de una red nacional de CSIRTs académicos y contribuir así a la investigación y desarrollo de metodologías y buenas prácticas que permitan mejorar la seguridad de las redes ecuatorianas.

Responsable: Responsable de sistemas y tecnologías de la información; y Responsable de Seguridad de la Información.

Duración: Debe empezar durante la fase de control de accesos. Se plantea dure 2 años.

Costes:

- Bien:

SISTEMA DE MONITOREO Y ALARMAS 5000 USD

Equipos 5000 USD

Mobiliario 2000 USD

- Servicio:

Consultoría 2000 USD

Capacitación 200 USD

Conectividad 2000 USD mensuales.

- Implantación: el 10% del sueldo del responsable de sistemas por 1 mes más el 40% del sueldo de un técnico de sistemas por 12 meses. Aproximadamente 9000 USD

Riesgo a mitigar:

[A.11] Ataques intencionados - Acceso no autorizado

[A.12] Ataques intencionados - Análisis de tráfico

[A.24] Ataques intencionados - Denegación de servicio

[A.25] Ataques intencionados - Robo

[A.5] Ataques intencionados - Suplantación de la identidad del usuario

[A.6] Ataques intencionados - Abuso de privilegios de acceso

[E.20] Errores y fallos no intencionados - Vulnerabilidades de los programas (software)

Impacto sobre los dominios de la seguridad: De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto ver el ANEXO IV.

En cuanto a la planificación temporal en la ejecución de los proyectos, tenemos lo siguiente:

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												

Cuadro 11: Plan de implementación de proyectos

4.3 Resultados

La propuesta de proyectos está alineada con el análisis del impacto “Capitulo 3”. Esto comporta, que su ejecución nos debe indicar cómo evoluciona el riesgo y el impacto de materialización, así como el nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC 27002.

Todos los proyectos planteados tienen un impacto positivo sobre todos los dominios de la seguridad. Comparando la situación encontrada al inicio del presente estudio y la situación una vez se implanten todos los proyectos propuestos, obtenemos la siguiente tabla de madurez, en porcentajes:

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%**

Cuadro 12: Impacto sobre el dominio de la seguridad después de implementado los proyectos

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%.

El detalle del impacto de los proyectos planteados en los diferentes dominios de la norma ISO/IEC27002:2013 se puede encontrar en el ANEXO IV.

Representando esta información en un gráfico de radar, se hace más evidente las mejoras sobre los dominios de la seguridad que implicaría la ejecución de los proyectos propuestos:

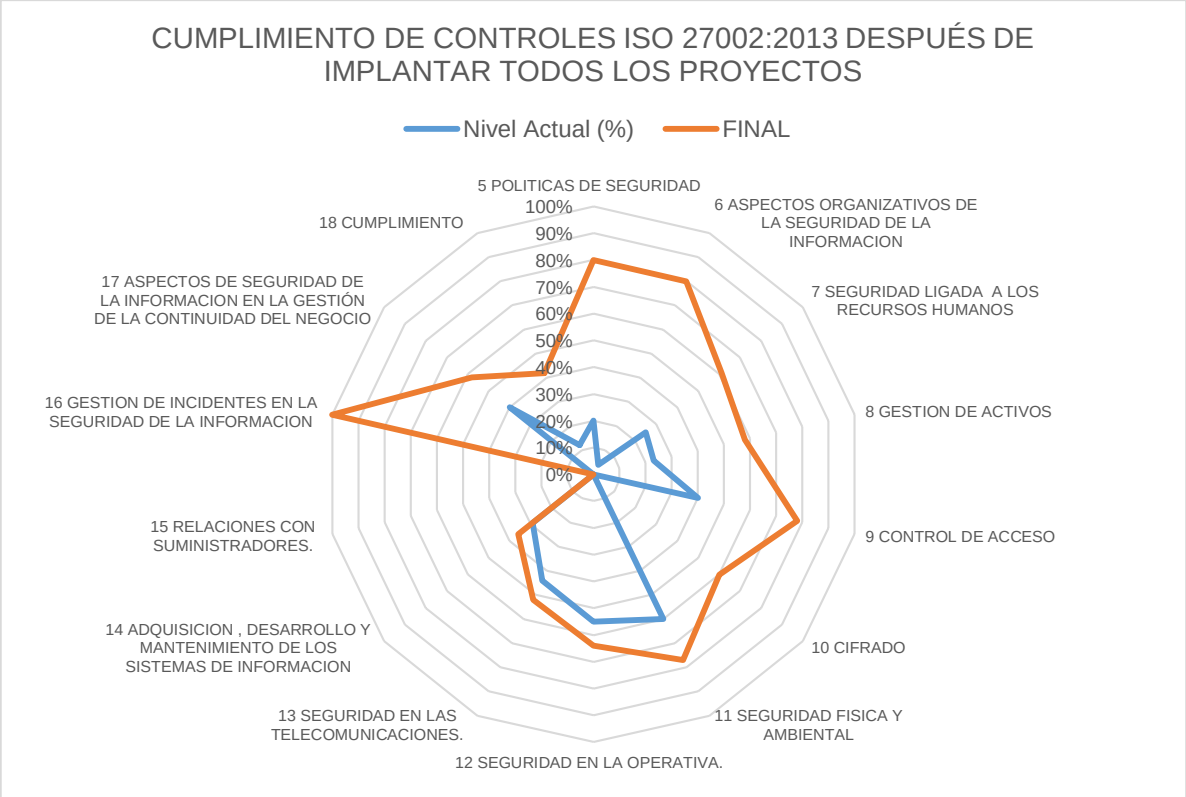

Gráfico 8: Cumplimiento de controles ISO 27002:2013 después de implantar los proyectos

5 Auditoría de Cumplimiento

5.1 Introducción

Llegados a esta fase, conocemos los activos de la empresa y hemos evaluado las amenazas. Es el momento de hacer un alto en el camino y evaluar hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad. La ISO/IEC 27002:2013 nos servirá como marco de control del estado de la seguridad.

5.2 Metodología

El estándar ISO/IEC 27002:2013, agrupa un total de 114 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 14 dominios y 35 objetivos de control. Éste estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de organizaciones.

Hay 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.

5.3 Evaluación de la madurez

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013. Antes de abordar intentaremos profundizar al máximo en el conocimiento de la organización.

De forma resumida, los dominios que deben analizarse son:

- Política de seguridad
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad en los recursos humanos

- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Gestión de incidentes
- Gestión de continuidad de negocio
- Cumplimiento

El estudio debe realizar una revisión de los 114 controles planteados por la norma para cumplir con los diferentes objetivos de control – el número de los cuales se indica entre paréntesis para cada uno de los dominios-. Esta estimación la realizaremos según la siguiente tabla, que se basa en el Modelo de Madurez de la Capacidad (CMM):

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.

Cuadro 13: Modelo de Madurez de la Capacidad (CMM)

A continuación, se muestra la valoración de madurez CMM tras la implantación de los proyectos propuestos:

Sección	Controles ISO 27002:2013	Justificación exclusión	Estimación	Madurez CMM (%)
5	Política de seguridad			**90%**
5.1.1	Conjunto de políticas para la seguridad de la información		Proceso definido	90%
5.1.2	Revisión de la Política de Seguridad de la Información		Proceso definido	90%
6	Aspectos Organización de la seguridad de la información			**82%**
6.1.1	Asignación de Responsabilidades para la Seguridad de la Información		Proceso definido	90%
6.1.2	Segregación de tareas.		Proceso definido	90%
6.1.3	Contacto con la Autoridades		Proceso definido	90%
6.1.4	Contacto con Grupos de Interés Especial		Reproducible, pero intuitivo	50%
6.1.5	Seguridad de la información en la gestión de proyectos.		Proceso definido	90%
6.2.1	Política de uso de dispositivos para movilidad.	La institución no cuenta con aplicaciones de informática móvil o de teletrabajo, para USB y portátiles se usa la política	Inexistente	NA

		de medios extraíbles		
6.2.2	Teletrabajo.	La institución no cuenta con aplicaciones de informática móvil o de teletrabajo.	Inexistente	NA
7	Seguridad ligada a los recursos humanos			50%
7.1.1	Investigación de Antecedentes		Reproducible, pero intuitivo	50%
7.1.2	Términos y condiciones de Contratación		Reproducible, pero intuitivo	50%
7.2.1	Responsabilidad de la gestión		Reproducible, pero intuitivo	50%
7.2.2	Concienciación. Formación y capacitación en seguridad de la información		Reproducible, pero intuitivo	50%
7.2.3	Procesos Disciplinario		Reproducible, pero intuitivo	50%
7.3.1	Cese o Cambio de Puesto de Trabajo		Reproducible, pero intuitivo	50%
8	Gestión de activos			**63%**
8.1.1	Inventario de Activos		Gestionado y medible	95%
8.1.2	Propiedad de los Activos		Proceso definido	90%
8.1.3	Uso aceptable de los Activos		Reproducible, pero intuitivo	50%
8.1.4	Devolución de activos		Reproducible, pero intuitivo	50%
8.2.1	Directrices de Clasificación		Reproducible, pero intuitivo	50%
8.2.2	Etiquetado y manipulación de la Información		Proceso definido	90%
8.2.3	Manipulación de activos		Reproducible, pero intuitivo	50%
8.3.1	Gestión de soportes extraíbles.		Reproducible, pero intuitivo	50%
8.3.2	Eliminación de soportes.		Reproducible, pero intuitivo	50%
8.3.3	Soportes físicos en tránsito.		Reproducible, pero intuitivo	50%
9	CONTROL DE ACCESO			**81%**
9.1.1	Política de Control de Acceso		Proceso definido	90%
9.1.2	Control de acceso a las redes y servicios asociados		Proceso definido	90%
9.2.1	Gestión de altas/bajas en el registro de usuarios.		Proceso definido	90%
9.2.2	Gestión de los derechos de acceso asignados a usuarios		Reproducible, pero intuitivo	50%
9.2.3	Gestión de los derechos de acceso con privilegios especiales.		Proceso definido	90%
9.2.4	Gestión de información confidencial de autenticación de usuarios.		Proceso definido	90%

9.2.5	Revisión de los derechos de acceso de los usuarios.		Reproducible, pero intuitivo	50%
9.2.6.	Retirada o adaptación de los derechos de acceso		Reproducible, pero intuitivo	50%
9.3.1	Uso de información confidencial para la autenticación		Proceso definido	90%
9.4.1	Restricción del acceso a la información.		Proceso definido	90%
9.4.2	Procedimientos seguros de inicio de sesión.		Proceso definido	90%
9.4.3	Gestión de contraseñas		Proceso definido	90%
9.4.4	Uso de herramientas de administración de sistemas		Proceso definido	90%
9.4.5	Control de acceso al código fuente de los programas		Proceso definido	90%
10	Cifrado			70%
10.1.1	Política de uso de los controles criptográficos		Proceso definido	90%
10.1.2	Gestión de claves		Reproducible, pero intuitivo	50%
11	Seguridad física y del entorno			85%
11.1.1	Perímetro de Seguridad Física		Proceso definido	90%
11.1.2	Controles Físicos de Entrada		Optimizado	100%
11.1.3	Seguridad de Oficinas, despachos e instalaciones		Optimizado	100%
11.1.4	Protección contra las amenazas eternas y de origen ambiental		Optimizado	100%
11.1.5	Trabajo en Áreas seguras		Gestionado y medible	95%
11.1.6	Áreas de acceso público, carga y descarga		Gestionado y medible	95%
11.2.1	Emplazamiento y protección de los equipos		Proceso definido	90%
11.2.2	Instalaciones de suministros		Proceso definido	90%
11.2.3	Seguridad del Cableado		Proceso definido	90%
11.2.4	Mantenimiento de los Equipos		Proceso definido	90%
11.2.5	Salida de activos fuera de las dependencias de la empresa.		Proceso definido	90%
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones		Reproducible, pero intuitivo	50%
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.		Reproducible, pero intuitivo	50%
11.2.8	Equipo informático de usuario desatendido		Reproducible, pero intuitivo	50%
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla		Proceso definido	90%
12	Seguridad en la Operatividad			84%
12.1.1	Documentación de los Procedimientos de Operación		Proceso definido	90%
12.1.2	Gestión de Cambios		Reproducible, pero intuitivo	50%

12.1.3	Gestión de capacidades.		Reproducible, pero intuitivo	50%
12.1.4	Separación de entornos de desarrollo, prueba y producción.		Proceso definido	90%
12.2.1	Controles contra el código malicioso		Optimizado	100%
12.3.1	Copias de Seguridad de la Información		Proceso definido	90%
12.4.1	Registro y gestión de eventos de actividad.		Proceso definido	90%
12.4.2	Protección de los registros Información		Proceso definido	90%
12.4.3	Registros de actividad del administrador y operador del sistema.		Proceso definido	90%
12.4.4	Sincronización del Reloj		Proceso definido	90%
12.5.1	Instalación del software en sistemas en producción.		Gestionado y medible	95%
12.6.1	Gestión de las vulnerabilidades técnicas.		Inicial / Ad-hoc	10%
12.6.2	Restricciones en la instalación de software.		Reproducible, pero intuitivo	50%
12.7.1	Controles de auditoría de los sistemas de información.		Inicial / Ad-hoc	10%
13	**Seguridad en las Telecomunicaciones**			85%
13.1.1	Controles de Red		Proceso definido	90%
13.1.2	Mecanismos de seguridad asociados a servicios en red.		Gestionado y medible	95%
13.1.3	Segregación de redes.		Proceso definido	90%
13.2.1	Políticas y Procedimientos de Intercambio de Información		Proceso definido	90%
13.2.2	Acuerdo de Intercambio		Reproducible, pero intuitivo	50%
13.2.3	Mensajería Electrónica		Proceso definido	90%
13.2.4	Acuerdos de confidencialidad y secreto.		Proceso definido	90%
14	Adquisición, desarrollo y mantenimiento de sistemas de información			56%
14.1.1	Análisis y especificaciones de los requisitos de seguridad		Reproducible, pero intuitivo	50%
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.		Reproducible, pero intuitivo	50%
14.1.3	Protección de las transacciones por redes telemáticas.		Proceso definido	90%
14.2.1	Política de desarrollo seguro de software.		Reproducible, pero intuitivo	50%
14.2.2	Procedimientos de control de cambios en los sistemas		Reproducible, pero intuitivo	50%
14.2.3	Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo		Reproducible, pero intuitivo	50%
14.2.4	Restricciones a los cambios en los paquetes de software		Reproducible, pero intuitivo	50%
14.2.5	Uso de principios de ingeniería en protección de sistemas.		Reproducible, pero intuitivo	50%
14.2.6	Seguridad en entornos de desarrollo.		Reproducible, pero intuitivo	50%

14.2.7	Externalización del Desarrollo del software		Reproducible, pero intuitivo	50%
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.		Reproducible, pero intuitivo	50%
14.2.9	Pruebas de aceptación.		Proceso definido	90%
14.3.1	Protección de los datos utilizados en pruebas.		Reproducible, pero intuitivo	50%
15	Relaciones con Suministradores			42%
15.1.1	Política de seguridad de la información para suministradores		Inicial / Ad-hoc	10%
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.		Inicial / Ad-hoc	10%
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.		Inicial / Ad-hoc	10%
15.2.1	Supervisión y revisión de los servicios prestados por terceros.		Proceso definido	90%
15.2.2	Gestión de cambios en los servicios prestados por terceros.		Proceso definido	90%
16	Gestión de incidentes de seguridad de la información			73%
16.1.1	Responsabilidades y Procedimientos		Proceso definido	90%
16.1.2	Notificación de los Eventos de Seguridad de la Información		Proceso definido	90%
16.1.3	Notificación de Puntos Débiles de la Seguridad		Proceso definido	90%
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.		Proceso definido	90%
16.1.5	Respuesta a los incidentes de seguridad.		Reproducible, pero intuitivo	50%
16.1.6	Aprendizaje de los incidentes de seguridad de la información.		Reproducible, pero intuitivo	50%
16.1.7	Recopilación de Evidencias		Reproducible, pero intuitivo	50%
17	Aspectos de Seguridad de la Información en la Gestión de continuidad del negocio			70%
17.1.1	Planificación de la continuidad de la seguridad de la información		Proceso definido	90%
17.1.2	Implantación de la continuidad de la seguridad de la información		Proceso definido	90%
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		Reproducible, pero intuitivo	50%
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.		Reproducible, pero intuitivo	50%
18	Cumplimiento			60%
18.1.1	Identificación de la legislación aplicable		Proceso definido	90%
18.1.2	Derechos de Propiedad Intelectual (DPI)		Reproducible, pero intuitivo	50%
18.1.3	Protección de los registros de la Organización		Reproducible, pero intuitivo	50%
18.1.4	Protección de Datos y privacidad de la información personal		Proceso definido	90%
18.1.5	Regulación de los Controles Criptográficos		Reproducible, pero intuitivo	50%

18.2.1	Revisión independiente de la seguridad de la información.		Reproducible, pero intuitivo	50%
18.2.2	Cumplimiento de las políticas y normas de seguridad		Reproducible, pero intuitivo	50%
18.2.3	Comprobación del cumplimiento.		Reproducible, pero intuitivo	50%

Cuadro 14: Valoración de madurez CMM del SGSI.

5.4 Presentación de resultados

Una vez realizada la valoración de la madurez de los 114 controles y 11 dominios de la norma empleada en la presente propuesta, podemos evidenciar que existe un 4% de controles que se encuentran en el nivel optimizado (**L5**), lo cual representa controles con una alta madurez, los cuales se gestionan, miden y controlan; un 4% de controles que se encuentran en el nivel gestionado y medible (**L4**), los mismos que son medidos, gestionados; un 11% de controles se encuentran en el nivel Inicial/Ad-Hoc (**L1**), lo cual se refiere que existen controles en procesos iniciales e incipientes de madurez y control; un 39% de controles se encuentran en el nivel Reproducible, pero intuitivo (**L2**), lo que representa que los controles se llevan a cabo de manera similar, pero aún no alcanzan un nivel de madurez donde se realice un seguimiento continuo y medible; y un 42% de controles se encuentran en el nivel Proceso definido (**L3**), lo cual nos indica que la entidad tiene controles con procedimientos adecuados y documentos, pero aun no mantienen indicadores y monitoreo sobre los mismos.

A continuación, se presenta una visión del estado de la seguridad en conjunto:

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**

Cuadro 15: Nivel de madurez CMM del SGSI.

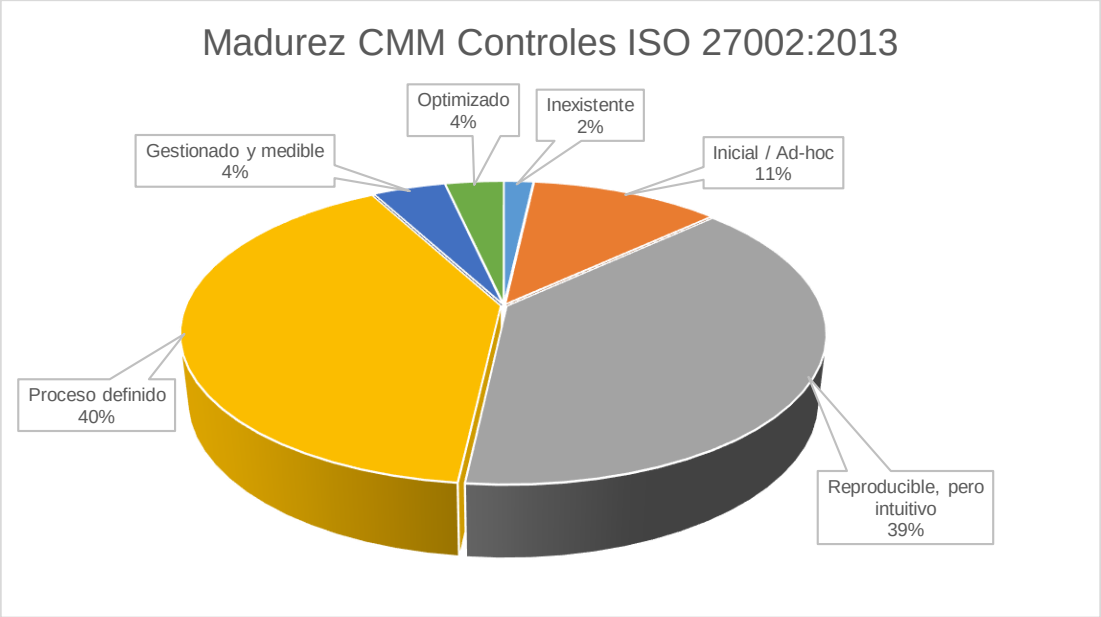

Gráfico 9: Madurez CMM Controles ISO 27002:2013

En el caso particular del caso en estudio, vemos que existe un porcentaje del 2% (Lo Inexistentes) son de 2 controles que no son aplicables.

Una visión más detallada es la que se presenta como 'diagrama de radar' que mostraría el nivel de cumplimiento por dominio ISO. Anticipándonos a las medidas, será interesante comparar el estado actual con el estado deseado, para más detalle ver el ANEXO III:

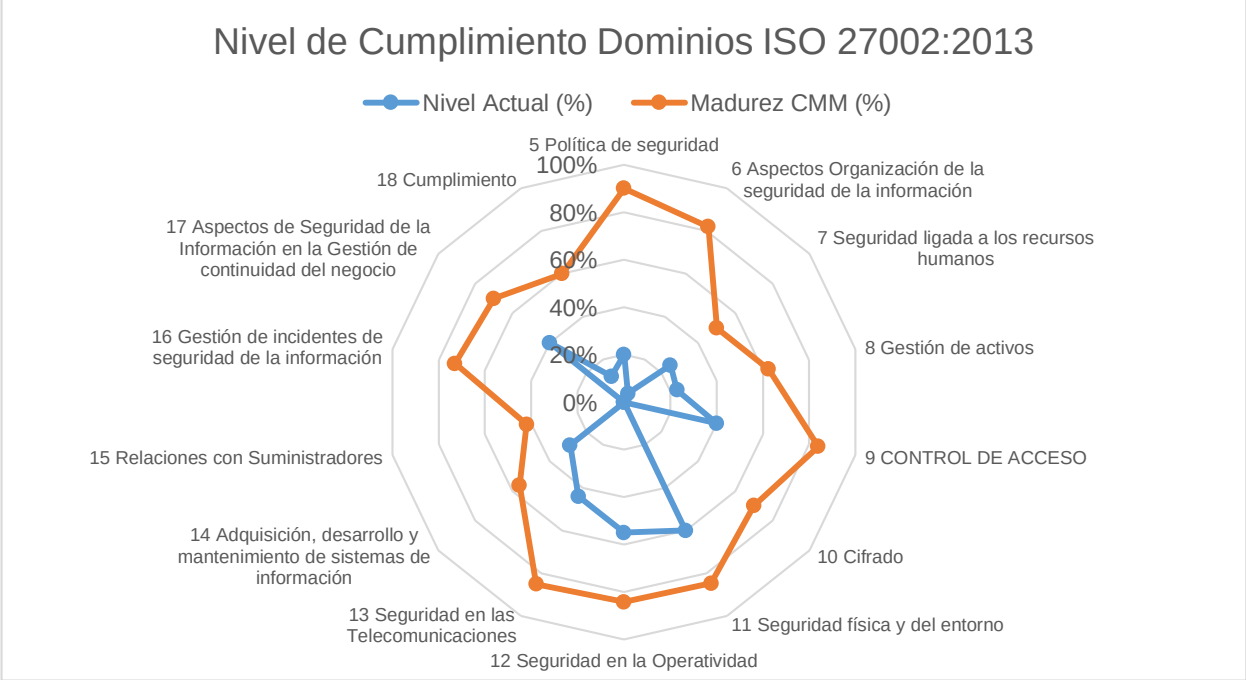

Gráfico 10: Nivel de Cumplimiento Dominios ISO 27002:2013

5.5 Resultados

Una vez completada esta fase, tenemos una visión del cumplimiento de los diferentes dominios de la ISO/IEC 27002:2013, para lo cual se tiene la siguiente clasificación:

- **No conformidad mayor:** Se incumple un apartado completo del estándar, por ejemplo, no se ha realizado un análisis de riesgos, o no se realizado la revisión por dirección, etc.
- **No conformidad menor:** Se incumple un punto de un apartado del estándar, por ejemplo, existe un análisis de riesgos, pero no se ha identificado un propietario del riesgo.
- **Observación:** No significa un incumplimiento del estándar, pero si no se hace un tratamiento adecuado, en el futuro se puede convertir en una no conformidad. Por ejemplo, La empresa ha realizado un análisis de riesgos, pero no ha establecido formalmente, en una agenda o calendario, cada cuanto tiempo revisará los resultados, y quién revisará los resultados.
- **Oportunidad de mejora:** No significa un incumplimiento del estándar, y si no se hace un tratamiento en el futuro no se convertirá en no conformidad. Por tanto, una oportunidad de mejora es simplemente una recomendación, que la empresa puede decidir no realizar.

Una vez realizada la auditoria de cumplimiento para los dominios de la ISO/IEC 27002:2013 se determina SGSI para la institución lo siguiente:

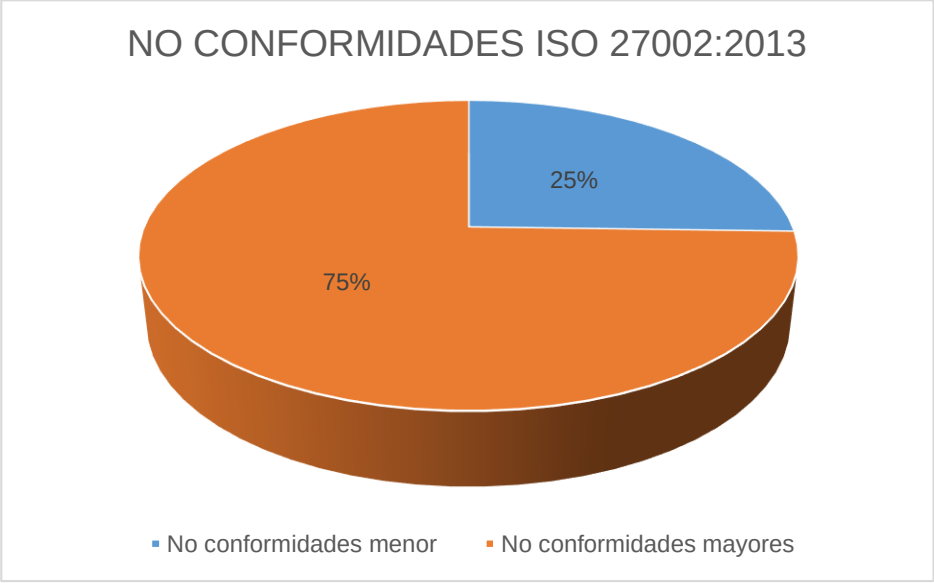

Gráfico 11: No Conformidades ISO 27002:2013

En la siguiente tabla se resume los diferentes dominios de la norma con el número de controles que no cumplen, las mismas que se han identificado las no conformidades mayores y menores:

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
	14	**41**

Cuadro 16: Cuadro de No Conformidades ISO 27002:2013

El detalle de las no conformidades se puede observar en el Anexo XII.

Se recomienda a la institución, generar planes de acción correctivos, con base a las no conformidades mayores y menores presentadas en SGSI, con el fin de cumplir con los requisitos exigidos en la norma ISO 27001:2013 (requisitos).

6 Conclusiones

- 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.
- Para el éxito del Plan de Seguridad de la Información se requiere de la participación y el compromiso de todos los miembros de la institución (estudiantes, docentes y personal administrativo) y principalmente de la Dirección.
- La Dirección es la encargada de garantizar el cumplimiento de los planes y objetivos de la seguridad del a información.
- 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 continuo.

7 Listado de Gráficos

8 Anexos

ANEXO I

OBJETIVOS DEL PLAN DIRECTOR E INFORME ANÁLISIS DIFERENCIAL

Objetivos del Plan Director

El Plan Director de Seguridad en sí mismo no tiene interés, ha de ir alineado con un objetivo estratégico que es el que va a delimitar el alcance del Plan Director de Seguridad.

En nuestro caso concreto, el alcance del Plan Director de Seguridad se va a enmarcar dentro de los principios y objetivos establecidos en el estatuto de la institución, de los cuales describimos a continuación:

- Principio de “Calidad. - La Universidad se regirá por los máximos estándares de excelencia en sus actividades y programas académicos, a fin de asegurar el mejoramiento continuo en todos sus niveles de formación, capacitación e investigación”
- Objetivo de “Los demás objetivos establecidos para la educación superior en la constitución de la República del Ecuador, la Ley Orgánica de Educación Superior, su Reglamento, el presente Estatuto y demás normativa aplicable”.

Basados en el objetivo anteriormente citado podemos establecer que la institución debe considerar:

Que, el numeral 2 del artículo 16 de la Constitución de la República del Ecuador establece como derecho de las personas, en forma individual o colectiva, el acceso universal a las tecnologías de información y comunicación;

Que, el numeral 21 del artículo 66 de la Constitución de la República del Ecuador reconoce y garantiza a las personas el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; derecho que protege cualquier otro tipo o forma de comunicación;

Que, el artículo 77 de la Ley Orgánica de la Contraloría General del Estado establece la obligación del Titular de la entidad de dirigir y asegurar la implantación, funcionamiento y actualización de los sistemas administrativos;

Que, el artículo 2 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos reconoce y otorga igual valor jurídico a los mensajes de datos que a los documentos físicos;

Que, el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, artículo 148 y Disposición Transitoria Décima Tercera, determina a las entidades contratantes del sector público orden de prelación en la contratación pública relacionada a software y un plan de migración a software libre;

Que, el Reglamento General para la administración, utilización, manejo y control de los bienes y existencias del sector público, considera, en su artículo 4, la reglamentación interna para la administración, uso, control y destino de los bienes del Estado; y en los artículos 103 y 104, disposiciones para el registro y mantenimiento de equipos informáticos, hardware y software;

Que, las Normas de Control Interno de la Contraloría General del Estado, Grupo 410 Tecnologías de la Información y Grupo 500 Información y Comunicación, regulan la información y la comunicación y su soporte tecnológico informático, con necesaria referencia a un modelo de información de la organización que facilite la creación, uso y compartición de la misma y garantice su disponibilidad, integridad, exactitud y seguridad, sobre la base de la definición e implantación de los procesos y procedimientos correspondientes;

Que, la Norma de Control Interno 410-04 Políticas y procedimientos, determina a la Unidad de Tecnología de Información definir, documentar y difundir políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, considerándose temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información; así mismo, la incorporación de controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos; y, la implantación de procedimientos de supervisión de las funciones de tecnología de información;

Que, la Norma de Control Interno 300-03 Valoración de los riesgos, determina "Se consideran factores de alto riesgo potencial los programas o actividades complejas... sistemas de información

rediseñados... nueva tecnología, entre otros. La valoración del riesgo se realiza usando el juicio profesional y la experiencia";

Se trata de un objetivo amplio que requiere la revisión de todos los sistemas de la institución y determinar qué puntos débiles existen en cada uno de ellos y realizar propuestas de mejoras puntuales y continuas.

Informe Análisis Diferencial

La siguiente tabla se muestra el resultado del análisis diferencial de las medidas de seguridad que la institución tiene actualmente implantadas respecto los requisitos que conforman la norma ISO 27002:2013:

No	Requisitos	Estado
4	**Contexto de la organización**	**18%**
4.1	Comprender la organización en su contexto	50%
4.2	Comprender las necesidades y expectativas de las partes interesadas	20%
4.3	Determinar el alcance del SGSI	0%
4.4	SGSI	0%
5	**Liderazgo**	**13%**
5.1	Liderazgo y compromiso	30%
5.2	Política	0%
5.3	Roles organizacionales, responsabilidades y autoridades=	10%
6	**Planificación**	0%
6.1	Acciones para abordar los riesgos y las oportunidades	0%
6.2	Objetivos de la seguridad de la información	0%
7	**Apoyo**	**6%**
7.1	Recursos	10%
7.2	Competencias	0%
7.3	Conocimiento	10%
7.4	Comunicación	0%

7.5	Información documentada	10%
8	**Operación**	**3%**
8.1	Control y planificación operacional	10%
8.2	Evaluación de riesgo de la SI	0%
8.3	Tratamiento del riesgo de la SI	0%
9	**Evaluación de desempeño**	**0%**
9.1	Monitoreo, medición, análisis y evaluación	0%
9.2	Auditoria interna	0%
9.3	Revisión de gestión	0%
10	**Mejora**	**0%**
10.1	No conformidades y acciones correctivas	0%
10.2	Mejora continua	0%

La siguiente tabla muestra el resultado del análisis diferencial de las medidas de seguridad que la institución tiene actualmente implantadas con respecto a los controles que conforman la norma ISO 27001:2013.

CONTROL	Nivel de Cumplimiento (%)
5 POLITICAS DE SEGURIDAD	**20%**
5.1 Directrices de la Dirección en seguridad de la información	20%
5.1.1 Conjunto de políticas para la seguridad de la información	20%
5.1.2 Revisión de la Política de Seguridad de la Información	20%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	**4%**
6.1 Organización Interna	8%
6.1.1 Asignación de Responsabilidades para la Seguridad de la Información	0%
6.1.2 Segregación de tareas.	20%
6.1.3 Contacto con la Autoridades	20%
6.1.4 Contacto con Grupos de Interés Especial	0%
6.1.5 Seguridad de la información en la gestión de proyectos.	0%
6.2 Dispositivos para movilidad y teletrabajo.	0%

6.2.1 Política de uso de dispositivos para movilidad.	0%
6.2.2 Teletrabajo.	0%
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**25%**
7.1 Antes de la contratación	35%
7.1.1 Investigación de Antecedentes	30%
7.1.2 Términos y condiciones de Contratación	40%
7.2 Durante la contratación	20%
7.2.1 Responsabilidad de la gestión	40%
7.2.2 Concienciación. Formación y capacitación en seguridad de la información	10%
7.2.3 Procesos Disciplinario	10%
7.3 Cese o Cambio de Puesto de Trabajo	20%
7.3.1 Cese o Cambio de Puesto de Trabajo	20%
8 GESTION DE ACTIVOS	**23%**
8.1 Responsabilidad Sobre Los Activos	60%
8.1.1 Inventario de Activos	90%
8.1.2 Propiedad de los Activos	50%
8.1.3 Uso aceptable de los Activos	50%
8.1.4 Devolución de activos	50%
8.2 Clasificación de la Información	10%
8.2.1 Directrices de Clasificación	0%
8.2.2 Etiquetado y manipulación de la Información	30%
8.2.3 Manipulación de activos	0%
8.3 Manejo de los soportes de almacenamiento.	0%
8.3.1 Gestión de soportes extraíbles.	0%
8.3.2 Eliminación de soportes.	0%
8.3.3 Soportes físicos en tránsito.	0%
9 CONTROL DE ACCESO	**40%**
9.1 Requisitos de Negocio para el Control de Acceso	55%
9.1.1 Política de Control de Acceso	30%
9.1.2 Control de acceso a las redes y servicios asociados	80%
9.2 Gestión de Acceso de Usuarios	23%

9.2.1 Gestión de altas/bajas en el registro de usuarios.	60%
9.2.2 Gestión de los derechos de acceso asignados a usuarios	20%
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	0%
9.2.4 Gestión de información confidencial de autenticación de usuarios.	40%
9.2.5 Revisión de los derechos de acceso de los usuarios.	0%
9.2.6 Retirada o adaptación de los derechos de acceso	20%
9.3 Responsabilidades de los Usuarios	20%
9.3.1 Uso de información confidencial para la autenticación	20%
9.4 Control de acceso a sistemas y aplicaciones.	62%
9.4.1 Restricción del acceso a la información.	40%
9.4.2 Procedimientos seguros de inicio de sesión.	80%
9.4.3 Gestión de contraseñas	80%
9.4.4 Uso de herramientas de administración de sistemas	60%
9.4.5 Control de acceso al código fuente de los programas	50%
10 CIFRADO	0%
10.1 Controles criptográficos	0%
10.1.1 Política de uso de los controles criptográficos	0%
10.1.2 Gestión de claves	0%
11 SEGURIDAD FISICA Y AMBIENTAL	**60%**
11.1 Áreas Seguras	88%
11.1.1 Perímetro de Seguridad Física	100%
11.1.2 Controles Físicos de Entrada	100%
11.1.3 Seguridad de Oficinas, despachos e instalaciones	100%
11.1.4 Protección contra las amenazas externas y de origen ambiental	90%
11.1.5 Trabajo en Áreas seguras	90%
11.1.6 Áreas de acceso público, carga y descarga	50%
11.2 Seguridad de los Equipos	32%
11.2.1 Emplazamiento y protección de los equipos	60%
11.2.2 Instalaciones de suministros	60%
11.2.3 Seguridad del Cableado	80%
11.2.4 Mantenimiento de los Equipos	90%
11.2.5 Salida de activos fuera de las dependencias de la empresa.	0%

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	0%
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	0%
11.2.8 Equipo informático de usuario desatendido	0%
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	0%
12 SEGURIDAD EN LA OPERATIVA.	55%
12.1 Responsabilidades y Procedimientos de Operación	25%
12.1.1 Documentación de los Procedimientos de Operación	40%
12.1.2 Gestión de Cambios	0%
12.1.3 Gestión de capacidades.	0%
12.1.4 Separación de entornos de desarrollo, prueba y producción.	60%
12.2 Protección contra Código Malicioso	100%
12.2.1 Controles contra el código malicioso	100%
12.3 Copias de Seguridad	60%
12.3.1 Copias de Seguridad de la Información	60%
12.4 Registro de actividad y supervisión.	68%
12.4.1 Registro y gestión de eventos de actividad.	60%
12.4.2 Protección de los registros Información	60%
12.4.3 Registros de actividad del administrador y operador del sistema.	60%
12.4.4 Sincronización del Reloj	90%
12.5 Control del software en explotación.	90%
12.5.1 Instalación del software en sistemas en producción.	90%
12.6 Gestión de la vulnerabilidad técnica	30%
12.6.1 Gestión de las vulnerabilidades técnicas.	40%
12.6.2 Restricciones en la instalación de software	20%
12.7 Consideraciones de las auditorías de los sistemas de información	10%
12.7.1 Controles de auditoría de los sistemas de información.	10%
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	**44%**
13.1 Gestión de Seguridad de las Redes	83%
13.1.1 Controles de Red	90%
13.1.2 Mecanismos de seguridad asociados a servicios en red.	80%
13.1.3 Intercambio de información con partes externas Segregación de redes.	80%

13.2 Intercambio de información con partes externas	5%
13.2.1 Políticas y Procedimientos de Intercambio de Información	0%
13.2.2 Acuerdo de Intercambio	0%
13.2.3 Mensajería Electrónica	0%
13.2.4 Acuerdos de confidencialidad y secreto.	20%
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	**29%**
14.1 Requisitos de Seguridad de los Sistemas de Información	67%
14.1.1 Análisis y especificaciones de los requisitos de seguridad	40%
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	80%
14.1.3 Protección de las transacciones por redes telemáticas.	80%
14.2 Seguridad en los procesos de Desarrollo y Soporte	20%
14.2.1 Política de desarrollo seguro de software.	0%
14.2.2 Procedimientos de control de cambios en los sistemas	0%
14.2.3 Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo	0%
14.2.4 Restricciones a los cambios en los paquetes de software	0%
14.2.5 Uso de principios de ingeniería en protección de sistemas.	20%
14.2.6 Seguridad en entornos de desarrollo.	0%
14.2.7 Externalización del Desarrollo del software	0%
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	80%
14.2.9 Pruebas de aceptación.	80%
14.3 Datos de prueba	0%
14.3.1 Protección de los datos utilizados en pruebas.	0%
15 RELACIONES CON SUMINISTRADORES.	**40%**
15.1 Seguridad de la información en las relaciones con suministradores	0%
15.1.1 Política de seguridad de la información para suministradores	0%
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	0%
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	0%
15.2 Gestión de la prestación del servicio por suministradores.	80%
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	80%

15.2.2 Gestión de cambios en los servicios prestados por terceros.	80%
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	**0%**
16.1 Gestión de Incidentes de Seguridad de la Información y Mejoras	0%
16.1.1 Responsabilidades y Procedimientos	0%
16.1.2 Notificación de los Eventos de Seguridad de la Información	0%
16.1.3 Notificación de Puntos Débiles de la Seguridad	0%
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	0%
16.1.5 Respuesta a los incidentes de seguridad.	0%
16.1.6 Aprendizaje de los Incidentes de Seguridad de la Información	0%
16.1.7 Recopilación de Evidencias	0%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**40%**
17.1 Continuidad de la seguridad de la información	0%
17.1.1 Planificación de la continuidad de la seguridad de la información	0%
17.1.2 Implantación de la continuidad de la seguridad de la información	0%
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	0%
17.2 Redundancias	80%
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	80%
18 CUMPLIMIENTO	**12%**
18.1 Cumplimiento de los requisitos legales y contractuales	24%
18.1.1 Identificación de la legislación aplicable	80%
18.1.2 Derechos de Propiedad Intelectual (DPI)	0%
18.1.3 Protección de los registros de la Organización	20%
18.1.4 Protección de Datos y privacidad de la información personal	20%
18.1.5 Regulación de los Controles Criptográficos	0%
18.2 Revisiones de la seguridad de la información.	0%
18.2.1 Revisión independiente de la seguridad de la información.	0%
18.2.2 Cumplimiento de las políticas y normas de seguridad	0%
18.2.3 Comprobación del cumplimiento.	0%

ANEXO 2

RESULTADOS DEL ANÁLISIS DE RIESGOS

Tabla de Impacto Potencial

Activo	Amenaza	Frecuencia	IMPACTO				
			A	C	I	D	T
Data Center - El Rosario	[N.*]	PR-MB				MA	
Data Center - El Rosario	[I.*]	PR-MB				MA	
Data Center - El Rosario	[I.6]	PR-B				MA	
Data Center - El Rosario	[A.11]	PR-MB		MA		MA	MA
Cuarto de Rack - San José	[N.*]	PR-MB				A	
Cuarto de Rack - San José	[I.*]	PR-MB				A	
Cuarto de Rack - San José	[I.6]	PR-B				A	
Cuarto de Rack - Ingenio - Principal	[N.*]	PR-MB				MA	
Cuarto de Rack - Ingenio - Principal	[I.*]	PR-MB				MA	
Cuarto de Rack - Ingenio - Principal	[I.6]	PR-B				MA	
Cuarto de Rack - Ingenio - Biblioteca	[N.*]	PR-MB				MA	
Cuarto de Rack - Ingenio - Biblioteca	[I.*]	PR-MB				MA	
Cuarto de Rack - Ingenio - Biblioteca	[I.6]	PR-B				MA	
Cuarto de Rack - Ingenio - Aulas	[N.*]	PR-MB				MA	
Cuarto de Rack - Ingenio - Aulas	[I.*]	PR-MB				MA	
Cuarto de Rack - Ingenio - Aulas	[I.6]	PR-B				MA	
Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[N.*]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[E.25]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[A.12]	PR-B				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[N.*]	PR-MB				A	

Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[E.25]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[A.12]	PR-B				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - Ingenio	[N.*]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - Ingenio	[E.25]	PR-MB				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - Ingenio	[A.12]	PR-B				A	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[N.*]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[E.25]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[A.14]	PR-B	M	M		M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[N.*]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[E.25]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[A.14]	PR-B	M	M		M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - Ingenio	[N.*]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - Ingenio	[E.25]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - Ingenio	[A.14]	PR-B	M	M		M	
Switch Core - El Rosario	[N.*]	PR-MB				MA	
Switch Core - El Rosario	[I.6]	PR-B				MA	
Switch Core - El Rosario	[I.7]	PR-MB				MA	
Switch Core - El Rosario	[E.28]	PR-B				MA	
Switch Core - El Rosario	[A.12]	PR-MB	MA	MA	MA	A	MA
Switch 24 puertos - El Rosario	[N.*]	PR-MB				A	
Switch 24 puertos - El Rosario	[I.6]	PR-B				A	
Switch 24 puertos - El Rosario	[I.7]	PR-MB				A	
Switch 24 puertos - El Rosario	[E.28]	PR-B				A	

Switch 24 puertos - El Rosario	[A.12]	PR-MB	A	A	A	B	A
Switch 24 puertos - Ingenio	[N.*]	PR-MB				A	
Switch 24 puertos - Ingenio	[I.6]	PR-B				A	
Switch 24 puertos - Ingenio	[I.7]	PR-MB				A	
Switch 24 puertos - Ingenio	[E.28]	PR-B				A	
Switch 24 puertos - Ingenio	[A.12]	PR-MB	A	A	A	B	A
Switch 48 puertos - El Rosario - Residencias	[N.*]	PR-MB				A	
Switch 48 puertos - El Rosario - Residencias	[I.6]	PR-B				A	
Switch 48 puertos - El Rosario - Residencias	[I.7]	PR-MB				A	
Switch 48 puertos - El Rosario - Residencias	[E.28]	PR-B				A	
Switch 48 puertos - El Rosario - Residencias	[A.12]	PR-MB	A	A	A	B	A
Switch 48 puertos - San José	[N.*]	PR-MB				A	
Switch 48 puertos - San José	[I.6]	PR-B				A	
Switch 48 puertos - San José	[I.7]	PR-MB				A	
Switch 48 puertos - San José	[E.28]	PR-B				A	
Switch 48 puertos - San José	[A.12]	PR-MB	A	A	A	B	A
Switch 48 puertos - Ingenio	[N.*]	PR-MB				A	
Switch 48 puertos - Ingenio	[I.6]	PR-B				A	
Switch 48 puertos - Ingenio	[I.7]	PR-MB				A	
Switch 48 puertos - Ingenio	[E.28]	PR-B				A	
Switch 48 puertos - Ingenio	[A.12]	PR-MB	A	A	A	B	A
Access Point - El Rosario	[N.*]	PR-MB				M	
Access Point - El Rosario	[I.6]	PR-B				M	
Access Point - El Rosario	[I.7]	PR-MB				M	
Access Point - El Rosario	[E.28]	PR-B				M	
Access Point - El Rosario	[A.12]	PR-MB	M	M	M	MB	M
Access Point - San José	[N.*]	PR-MB				M	
Access Point - San José	[I.6]	PR-B				M	
Access Point - San José	[I.7]	PR-MB				M	

Access Point - San José	[E.28]	PR-B				M	
Access Point - San José	[A.12]	PR-MB	M	M	M	MB	M
Access Point - Ingenio	[N.*]	PR-MB				M	
Access Point - Ingenio	[I.6]	PR-B				M	
Access Point - Ingenio	[I.7]	PR-MB				M	
Access Point - Ingenio	[E.28]	PR-B				M	
Access Point - Ingenio	[A.12]	PR-MB	M	M	M	MB	M
Routers Inalambricos - El Rosario	[N.*]	PR-MB				M	
Routers Inalambricos - El Rosario	[I.6]	PR-B				M	
Routers Inalambricos - El Rosario	[I.7]	PR-MB				M	
Routers Inalambricos - El Rosario	[E.28]	PR-B				M	
Routers Inalambricos - El Rosario	[A.12]	PR-MB	M	M	M	MB	M
Routers Inalambricos - San José	[N.*]	PR-MB				M	
Routers Inalambricos - San José	[I.6]	PR-B				M	
Routers Inalambricos - San José	[I.7]	PR-MB				M	
Routers Inalambricos - San José	[E.28]	PR-B				M	
Routers Inalambricos - San José	[A.12]	PR-MB	M	M	M	MB	M
Routers Inalambricos - Ingenio	[N.*]	PR-MB				M	
Routers Inalambricos - Ingenio	[I.6]	PR-B				M	
Routers Inalambricos - Ingenio	[I.7]	PR-MB				M	
Routers Inalambricos - Ingenio	[E.28]	PR-B				M	
Routers Inalambricos - Ingenio	[A.12]	PR-MB	M	M	M	MB	M
Firewall - El Rosario	[N.*]	PR-MB				MA	
Firewall - El Rosario	[I.6]	PR-B				MA	
Firewall - El Rosario	[I.7]	PR-MB				MA	
Firewall - El Rosario	[A.11]	PR-MB	MA	MA	MA	MA	MA
Firewall - El Rosario	[A.24]	PR-MB				MA	
Routers - El Rosario	[N.*]	PR-MB				MA	
Routers - El Rosario	[I.6]	PR-B				MA	
Routers - El Rosario	[I.7]	PR-MB				MA	
Routers - El Rosario	[E.28]	PR-B				MA	
Routers - El Rosario	[A.12]	PR-MB	MA	MA	MA	M	MA

Computadores de Escritorio - San José - Ingenio	[N.*]	PR-MB				M	
Computadores de Escritorio - San José - Ingenio	[I.1]	PR-MB				M	
Computadores de Escritorio - San José - Ingenio	[I.2]	PR-MB				M	
Computadores de Escritorio - San José - Ingenio	[I.6]	PR-MB				M	
Computadores de Escritorio - San José - Ingenio	[E.1]	PR-B		B	M		
Computadores de Escritorio - San José - Ingenio	[E.4]	PR-M				M	
Computadores Todo en Uno - Ingenio	[N.*]	PR-MB				B	
Computadores Todo en Uno - Ingenio	[I.1]	PR-MB				B	
Computadores Todo en Uno - Ingenio	[I.2]	PR-MB				B	
Computadores Todo en Uno - Ingenio	[I.6]	PR-MB				B	
Computadores Todo en Uno - Ingenio	[E.1]	PR-B		MB	B		
Computadores Todo en Uno - Ingenio	[E.4]	PR-M				B	
Portátiles - San José - Ingenio	[N.*]	PR-MB				M	
Portátiles - San José - Ingenio	[I.1]	PR-MB				M	
Portátiles - San José - Ingenio	[I.2]	PR-MB				M	
Portátiles - San José - Ingenio	[I.6]	PR-MB				M	
Portátiles - San José - Ingenio	[E.1]	PR-B		B	M		
Portátiles - San José - Ingenio	[E.4]	PR-M				M	
Portátiles - San José - Ingenio	[E.25]	PR-MB	MB	M	MB	M	
Portátiles - San José - Ingenio	[A.25]	PR-B	MB	M	MB	M	
Apple MAC ProBook - San José	[N.*]	PR-MB				B	
Apple MAC ProBook - San José	[I.1]	PR-MB				B	
Apple MAC ProBook - San José	[I.2]	PR-MB				B	
Apple MAC ProBook - San José	[I.6]	PR-MB				B	
Apple MAC ProBook - San José	[E.1]	PR-B		MB	B		
Apple MAC ProBook - San José	[E.4]	PR-M				B	
Apple MAC ProBook - San José	[E.25]	PR-MB	MB	B	MB	B	
Apple MAC ProBook - San José	[A.25]	PR-B	MB	B	MB	B	
Impresoras - El Rosario	[N.*]	PR-MB				A	

Impresoras - El Rosario	[I.1]	PR-MB				A	
Impresoras - El Rosario	[I.2]	PR-MB				A	
Impresoras - El Rosario	[I.6]	PR-M				A	
Impresoras - El Rosario	[E.1]	PR-M				A	
Impresoras - El Ingenio	[N.*]	PR-MB				A	
Impresoras - El Ingenio	[I.1]	PR-MB				A	
Impresoras - El Ingenio	[I.2]	PR-MB				A	
Impresoras - El Ingenio	[I.6]	PR-M				A	
Impresoras - El Ingenio	[E.1]	PR-M				A	
Impresoras - San José	[N.*]	PR-MB				A	
Impresoras - San José	[I.1]	PR-MB				A	
Impresoras - San José	[I.2]	PR-MB				A	
Impresoras - San José	[I.6]	PR-M				A	
Impresoras - San José	[E.1]	PR-M				A	
Teléfonos IP - El Rosario	[N.*]	PR-MB				M	
Teléfonos IP - El Rosario	[I.1]	PR-MB				M	
Teléfonos IP - El Rosario	[I.2]	PR-MB				M	
Teléfonos IP - El Rosario	[A.25]	PR-MB				M	
Teléfonos IP - San José	[N.*]	PR-MB				M	
Teléfonos IP - San José	[I.1]	PR-MB				M	
Teléfonos IP - San José	[I.2]	PR-MB				M	
Teléfonos IP - San José	[A.25]	PR-MB				M	
Teléfonos IP - Ingenio	[N.*]	PR-MB				M	
Teléfonos IP - Ingenio	[I.1]	PR-MB				M	
Teléfonos IP - Ingenio	[I.2]	PR-MB				M	
Teléfonos IP - Ingenio	[A.25]	PR-MB				M	
Lectores de tarjetas de proximidad - El Rosario	[N.*]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Rosario	[I.1]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Rosario	[I.2]	PR-B				MA	

Lectores de tarjetas de proximidad - El Rosario	[I.6]	PR-M				MA	
Lectores de tarjetas de proximidad - El Rosario	[A.23]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Rosario	[A.25]	PR-MB				MA	
Lectores de tarjetas de proximidad - San José	[N.*]	PR-MB				MA	
Lectores de tarjetas de proximidad - San José	[I.1]	PR-MB				MA	
Lectores de tarjetas de proximidad - San José	[I.2]	PR-B				MA	
Lectores de tarjetas de proximidad - San José	[I.6]	PR-M				MA	
Lectores de tarjetas de proximidad - San José	[A.23]	PR-MB				MA	
Lectores de tarjetas de proximidad - San José	[A.25]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[N.*]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.1]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.2]	PR-B				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.6]	PR-M				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[A.23]	PR-MB				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[A.25]	PR-MB				MA	
Servidores - El Rosario	[N.*]	PR-MB				MA	
Servidores - El Rosario	[I.6]	PR-M				MA	
Servidores - El Rosario	[I.7]	PR-B				MA	
Servidores - El Rosario	[E.2]	PR-MB				MA	
Servidores - El Rosario	[E.23]	PR-MB	MA			MA	A
Servidores - El Rosario	[A.6]	PR-MB				MA	A
NAS - El Rosario	[N.*]	PR-MB				M	

NAS - El Rosario	[I.6]	PR-M				M	
NAS - El Rosario	[I.7]	PR-B				M	
NAS - El Rosario	[E.2]	PR-MB				M	
NAS - El Rosario	[E.23]	PR-MB	M			M	B
NAS - El Rosario	[A.6]	PR-MB				M	B
Ofimática - Toda la Institución	[E.20]	PR-MB		M	M	M	
Ofimática - Toda la Institución	[E.21]	PR-B				M	B
Sistema Operativo Cliente - Toda la Institución	[E.20]	PR-MB		M	M	M	
Sistema Operativo Cliente - Toda la Institución	[E.21]	PR-B				M	B
Sistema Operativo Cliente - Toda la Institución	[A.11]	PR-MB	M	M	M	M	M
Motor de Base de Datos - Servicios de Gestión Académica.	[E.20]	PR-MB		MA	MA	MA	
Motor de Base de Datos - Servicios de Gestión Académica.	[E.21]	PR-B				MA	MA
Motor de Base de Datos - Servicios de Gestión Académica.	[A.6]	PR-MB	MA	MA	MA	MA	MA
Motor de Base de Datos - Servicios de Gestión Académica.	[A.11]	PR-MB	MA	MA	MA	MA	MA
Sistema Operativo Servidores - Toda la Institución	[E.20]	PR-MB		A	A	A	
Sistema Operativo Servidores - Toda la Institución	[E.21]	PR-B				A	M
Sistema Operativo Servidores - Toda la Institución	[A.6]	PR-MB	A	A	A	A	A
Sistema Operativo Servidores - Toda la Institución	[A.11]	PR-MB	A	A	A	A	A
Licencia de Escritorio Remoto - Dispositivo - Servicios de Gestión Académica.	[A.25]	PR-MB				A	
Aplicaciones de Desarrollo - Servicios de Gestión Académica.	[A.25]	PR-MB				A	
Servidor de Terminal Services - Servicios de Gestión Académica.	[E.20]	PR-MB	A	A	A	A	B
Servidor de Terminal Services - Servicios de Gestión Académica.	[E.21]	PR-B				A	M

Servidor de Terminal Services - Servicios de Gestión Académica.	[A.6]	PR-MB	A	A	A	A	A
Servidor de Terminal Services - Servicios de Gestión Académica.	[A.11]	PR-MB	A	A	A	A	A
Servidor de Terminal Services - Servicios de Gestión Académica.	[E.2]	PR-MB	A	A	A	A	A
Servidor Directorio Activo - Toda la Institución	[E.20]	PR-MB	MA	MA	MA	MA	A
Servidor Directorio Activo - Toda la Institución	[E.21]	PR-B				MA	MA
Servidor Directorio Activo - Toda la Institución	[A.6]	PR-MB	MA	MA	MA	MA	MA
Servidor Directorio Activo - Toda la Institución	[A.11]	PR-MB	MA	MA	MA	MA	MA
Servidor Directorio Activo - Toda la Institución	[E.2]	PR-MB	MA	MA	MA	MA	MA
Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.20]	PR-MB	MA	MA	MA	MA	M
Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.21]	PR-B				MA	A
Servidor de Aplicaciones - Servicios de Gestión Académica.	[A.6]	PR-MB	MA	MA	MA	MA	MA
Servidor de Aplicaciones - Servicios de Gestión Académica.	[A.11]	PR-MB	MA	MA	MA	MA	MA
Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.2]	PR-MB	MA	MA	MA	MA	MA
Licencia de Antivirus Clientes - Toda la Institución	[A.25]	PR-MB				A	B
Servidor DHCP - Toda la Institución	[E.20]	PR-MB	MA			MA	M
Servidor DHCP - Toda la Institución	[E.21]	PR-B				MA	A
Servidor DHCP - Toda la Institución	[A.6]	PR-MB	MA			MA	MA
Servidor DHCP - Toda la Institución	[A.11]	PR-MB	MA			MA	MA
Servidor DHCP - Toda la Institución	[E.2]	PR-MB	MA			MA	MA
Servidor Antivirus - Toda la Institución	[E.20]	PR-MB	A			A	B
Servidor Antivirus - Toda la Institución	[E.21]	PR-B				A	M
Servidor Antivirus - Toda la Institución	[A.6]	PR-MB	A			A	A
Servidor Antivirus - Toda la Institución	[A.11]	PR-MB	A			A	A

Servidor Antivirus - Toda la Institución	[E.2]	PR-MB	A			A	A
Servidor de Backup MV - Toda la Institución	[E.20]	PR-MB	MA	MA	MA	MA	M
Servidor de Backup MV - Toda la Institución	[E.21]	PR-B				MA	A
Servidor de Backup MV - Toda la Institución	[A.6]	PR-MB	MA	MA	MA	MA	MA
Servidor de Backup MV - Toda la Institución	[A.11]	PR-MB	MA	MA	MA	MA	MA
Servidor de Backup MV - Toda la Institución	[E.2]	PR-MB	MA	MA	MA	MA	MA
Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.20]	PR-MB	MA	MA	MA	MA	A
Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.21]	PR-B				MA	MA
Servidor de Backup Archivos - Servicios de Gestión Académica.	[A.6]	PR-MB	MA	MA	MA	MA	MA
Servidor de Backup Archivos - Servicios de Gestión Académica.	[A.11]	PR-MB	MA	MA	MA	MA	MA
Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.2]	PR-MB	MA	MA	MA	MA	MA
Base de Datos Estudiantes - Servicios de Gestión Académica.	[E.1]	PR-B		MA	MA	MA	MA
Base de Datos Estudiantes - Servicios de Gestión Académica.	[E.15]	PR-B		A	MA	MA	MA
Base de Datos Estudiantes - Servicios de Gestión Académica.	[A.11]	PR-MB	MA	MA	MA	MA	MA
Base de Datos Docentes - Servicios de Gestión Académica.	[E.1]	PR-B		MA	MA	MA	MA
Base de Datos Docentes - Servicios de Gestión Académica.	[E.15]	PR-B		A	MA	MA	MA
Base de Datos Docentes - Servicios de Gestión Académica.	[A.11]	PR-MB	MA	MA	MA	MA	MA
Base de Datos Personal Administrativo - Toda la Institución	[E.1]	PR-B		MA	MA	MA	MA
Base de Datos Personal Administrativo - Toda la Institución	[E.15]	PR-B		A	MA	MA	MA
Base de Datos Personal Administrativo - Toda la Institución	[A.11]	PR-MB	MA	MA	MA	MA	MA

Estudiantes - Toda la Institución	[A.5]	PR-MB		MA			
Estudiantes - Toda la Institución	[E.28]	PR-MB				MA	
Docentes - Toda la Institución	[A.5]	PR-MB	MA	MA	MA	MA	
Docentes - Toda la Institución	[E.28]	PR-MB				MA	
Personal Administrativo - Toda la Institución	[E.28]	PR-MB				A	
Personal Administrativo - Toda la Institución	[A.28]	PR-MB				A	
Personal Administrativo - Toda la Institución	[A.30]	PR-MB		A			A
Administrador de Infraestructura - Toda la Institución	[E.28]	PR-MB				MA	
Administrador de Infraestructura - Toda la Institución	[A.28]	PR-MB				MA	
Administrador de Infraestructura - Toda la Institución	[A.30]	PR-MB		MA			MA
Administrador Base de Datos - Toda la Institución	[E.28]	PR-MB				MA	
Administrador Base de Datos - Toda la Institución	[A.28]	PR-MB				MA	
Administrador Base de Datos - Toda la Institución	[A.30]	PR-MB		MA			MA
Correo Electrónico - Google Suite	[I.8]	PR-MB				A	
Correo Electrónico - Google Suite	[E.2]	PR-MB	M	A	A	A	A
Correo Electrónico - Google Suite	[A.24]	PR-MB				A	
Herramienta Colaborativa - Google Suite	[I.8]	PR-MB				M	
Herramienta Colaborativa - Google Suite	[E.2]	PR-MB	B	M	M	M	M
Herramienta Colaborativa - Google Suite	[A.24]	PR-MB				M	
IaaS - CNT	[I.8]	PR-MB				MA	
IaaS - CNT	[E.2]	PR-MB	MA	MA	MA	MA	MA
IaaS - CNT	[A.24]	PR-MB				MA	
Sistema Académico - Power Campus - Front End	[I.8]	PR-MB				MA	
Sistema Académico - Power Campus - Front End	[E.1]	PR-MB	MA	MA	MA	MA	MA

Sistema Académico - Power Campus - Front End	[A.24]	PR-MB				MA	
Sistema Académico - Power Campus - Back End	[I.8]	PR-MB				MA	
Sistema Académico - Power Campus - Back End	[E.2]	PR-MB	MA	MA	MA	MA	MA
Sistema Académico - Power Campus - Back End	[A.24]	PR-MB				MA	
Sistema Virtual de Aprendizaje - D2L - Front End	[I.8]	PR-MB				MA	
Sistema Virtual de Aprendizaje - D2L - Front End	[E.1]	PR-MB	MA	MA	MA	A	MA
Sistema Virtual de Aprendizaje - D2L - Front End	[A.24]	PR-MB				MA	
Sistema Virtual de Aprendizaje - D2L - Back End	[I.8]	PR-MB				MA	
Sistema Virtual de Aprendizaje - D2L - Back End	[E.2]	PR-MB	MA	MA	MA	MA	MA
Sistema Virtual de Aprendizaje - D2L - Back End	[A.24]	PR-MB				MA	
Usuario Externo -	[E.28]	PR-MB				MA	
Usuario Interno -	[E.28]	PR-MB				MA	

Tabla de Riesgo Potencial

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	
Puntos de Red – Cableado Estructurado – Servidores - El Rosario	[A.12]	PR-B				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[N.*]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[E.25]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - San José	[A.12]	PR-B				A	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - Ingenio	[N.*]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - Ingenio	[E.25]	PR-MB				M	
Puntos de Red – Cableado Estructurado – Puestos de Trabajo - Ingenio	[A.12]	PR-B				A	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[N.*]	PR-MB				B	

Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[E.25]	PR-MB				B	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - El Rosario	[A.14]	PR-B	M	M		M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[N.*]	PR-MB				B	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[E.25]	PR-MB				B	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - San José	[A.14]	PR-B	M	M		M	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - Ingenio	[N.*]	PR-MB				B	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - Ingenio	[E.25]	PR-MB				B	
Puntos de Red – Cableado Estructurado – Dispositivos de Red - Ingenio	[A.14]	PR-B	M	M		M	
Switch Core - El Rosario	[N.*]	PR-MB				A	
Switch Core - El Rosario	[I.6]	PR-B				MA	
Switch Core - El Rosario	[I.7]	PR-MB				A	
Switch Core - El Rosario	[E.28]	PR-B				MA	
Switch Core - El Rosario	[A.12]	PR-MB	A	A	A	M	A
Switch 24 puertos - El Rosario	[N.*]	PR-MB				M	
Switch 24 puertos - El Rosario	[I.6]	PR-B				A	
Switch 24 puertos - El Rosario	[I.7]	PR-MB				M	
Switch 24 puertos - El Rosario	[E.28]	PR-B				A	
Switch 24 puertos - El Rosario	[A.12]	PR-MB	M	M	M	MB	M
Switch 24 puertos - Ingenio	[N.*]	PR-MB				M	
Switch 24 puertos - Ingenio	[I.6]	PR-B				A	
Switch 24 puertos - Ingenio	[I.7]	PR-MB				M	
Switch 24 puertos - Ingenio	[E.28]	PR-B				A	

Switch 24 puertos - Ingenio	[A.12]	PR-MB	M	M	M	MB	M
Switch 48 puertos - El Rosario - Residencias	[N.*]	PR-MB				M	
Switch 48 puertos - El Rosario - Residencias	[I.6]	PR-B				A	
Switch 48 puertos - El Rosario - Residencias	[I.7]	PR-MB				M	
Switch 48 puertos - El Rosario - Residencias	[E.28]	PR-B				A	
Switch 48 puertos - El Rosario - Residencias	[A.12]	PR-MB	M	M	M	MB	M
Switch 48 puertos - San José	[N.*]	PR-MB				M	
Switch 48 puertos - San José	[I.6]	PR-B				A	
Switch 48 puertos - San José	[I.7]	PR-MB				M	
Switch 48 puertos - San José	[E.28]	PR-B				A	
Switch 48 puertos - San José	[A.12]	PR-MB	M	M	M	MB	M
Switch 48 puertos - Ingenio	[N.*]	PR-MB				M	
Switch 48 puertos - Ingenio	[I.6]	PR-B				A	
Switch 48 puertos - Ingenio	[I.7]	PR-MB				M	
Switch 48 puertos - Ingenio	[E.28]	PR-B				A	
Switch 48 puertos - Ingenio	[A.12]	PR-MB	M	M	M	MB	M
Access Point - El Rosario	[N.*]	PR-MB				B	
Access Point - El Rosario	[I.6]	PR-B				M	
Access Point - El Rosario	[I.7]	PR-MB				B	
Access Point - El Rosario	[E.28]	PR-B				M	
Access Point - El Rosario	[A.12]	PR-MB	B	B	B	MB	B
Access Point - San José	[N.*]	PR-MB				B	
Access Point - San José	[I.6]	PR-B				M	
Access Point - San José	[I.7]	PR-MB				B	
Access Point - San José	[E.28]	PR-B				M	
Access Point - San José	[A.12]	PR-MB	B	B	B	MB	B
Access Point - Ingenio	[N.*]	PR-MB				B	
Access Point - Ingenio	[I.6]	PR-B				M	
Access Point - Ingenio	[I.7]	PR-MB				B	

Access Point - Ingenio	[E.28]	PR-B				M	
Access Point - Ingenio	[A.12]	PR-MB	B	B	B	MB	B
Routers Inalambricos - El Rosario	[N.*]	PR-MB				B	
Routers Inalambricos - El Rosario	[I.6]	PR-B				M	
Routers Inalambricos - El Rosario	[I.7]	PR-MB				B	
Routers Inalambricos - El Rosario	[E.28]	PR-B				M	
Routers Inalambricos - El Rosario	[A.12]	PR-MB	B	B	B	MB	B
Routers Inalambricos - San José	[N.*]	PR-MB				B	
Routers Inalambricos - San José	[I.6]	PR-B				M	
Routers Inalambricos - San José	[I.7]	PR-MB				B	
Routers Inalambricos - San José	[E.28]	PR-B				M	
Routers Inalambricos - San José	[A.12]	PR-MB	B	B	B	MB	B
Routers Inalambricos - Ingenio	[N.*]	PR-MB				B	
Routers Inalambricos - Ingenio	[I.6]	PR-B				M	
Routers Inalambricos - Ingenio	[I.7]	PR-MB				B	
Routers Inalambricos - Ingenio	[E.28]	PR-B				M	
Routers Inalambricos - Ingenio	[A.12]	PR-MB	B	B	B	MB	B
Firewall - El Rosario	[N.*]	PR-MB				A	
Firewall - El Rosario	[I.6]	PR-B				MA	
Firewall - El Rosario	[I.7]	PR-MB				A	
Firewall - El Rosario	[A.11]	PR-MB	A	A	A	A	A
Firewall - El Rosario	[A.24]	PR-MB				A	
Routers - El Rosario	[N.*]	PR-MB				A	
Routers - El Rosario	[I.6]	PR-B				MA	
Routers - El Rosario	[I.7]	PR-MB				A	
Routers - El Rosario	[E.28]	PR-B				MA	
Routers - El Rosario	[A.12]	PR-MB	A	A	A	B	A
Computadores de Escritorio - San José - Ingenio	[N.*]	PR-MB				B	
Computadores de Escritorio - San José - Ingenio	[I.1]	PR-MB				B	
Computadores de Escritorio - San José - Ingenio	[I.2]	PR-MB				B	

Computadores de Escritorio - San José - Ingenio	[I.6]	PR-MB				B	
Computadores de Escritorio - San José - Ingenio	[E.1]	PR-B		B	M		
Computadores de Escritorio - San José - Ingenio	[E.4]	PR-M				M	
Computadores Todo en Uno - Ingenio	[N.*]	PR-MB				MB	
Computadores Todo en Uno - Ingenio	[I.1]	PR-MB				MB	
Computadores Todo en Uno - Ingenio	[I.2]	PR-MB				MB	
Computadores Todo en Uno - Ingenio	[I.6]	PR-MB				MB	
Computadores Todo en Uno - Ingenio	[E.1]	PR-B		MB	B		
Computadores Todo en Uno - Ingenio	[E.4]	PR-M				B	
Portátiles - San José - Ingenio	[N.*]	PR-MB				B	
Portátiles - San José - Ingenio	[I.1]	PR-MB				B	
Portátiles - San José - Ingenio	[I.2]	PR-MB				B	
Portátiles - San José - Ingenio	[I.6]	PR-MB				B	
Portátiles - San José - Ingenio	[E.1]	PR-B		B	M		
Portátiles - San José - Ingenio	[E.4]	PR-M				M	
Portátiles - San José - Ingenio	[E.25]	PR-MB	MB	B	MB	B	
Portátiles - San José - Ingenio	[A.25]	PR-B	MB	M	MB	M	
Apple MAC ProBook - San José	[N.*]	PR-MB				MB	
Apple MAC ProBook - San José	[I.1]	PR-MB				MB	
Apple MAC ProBook - San José	[I.2]	PR-MB				MB	
Apple MAC ProBook - San José	[I.6]	PR-MB				MB	
Apple MAC ProBook - San José	[E.1]	PR-B		MB	B		
Apple MAC ProBook - San José	[E.4]	PR-M				B	
Apple MAC ProBook - San José	[E.25]	PR-MB	MB	MB	MB	MB	
Apple MAC ProBook - San José	[A.25]	PR-B	MB	B	MB	B	
Impresoras - El Rosario	[N.*]	PR-MB				M	
Impresoras - El Rosario	[I.1]	PR-MB				M	

Impresoras - El Rosario	[I.2]	PR-MB				M	
Impresoras - El Rosario	[I.6]	PR-M				A	
Impresoras - El Rosario	[E.1]	PR-M				A	
Impresoras - El Ingenio	[N.*]	PR-MB				M	
Impresoras - El Ingenio	[I.1]	PR-MB				M	
Impresoras - El Ingenio	[I.2]	PR-MB				M	
Impresoras - El Ingenio	[I.6]	PR-M				A	
Impresoras - El Ingenio	[E.1]	PR-M				A	
Impresoras - San José	[N.*]	PR-MB				M	
Impresoras - San José	[I.1]	PR-MB				M	
Impresoras - San José	[I.2]	PR-MB				M	
Impresoras - San José	[I.6]	PR-M				A	
Impresoras - San José	[E.1]	PR-M				A	
Teléfonos IP - El Rosario	[N.*]	PR-MB				B	
Teléfonos IP - El Rosario	[I.1]	PR-MB				B	
Teléfonos IP - El Rosario	[I.2]	PR-MB				B	
Teléfonos IP - El Rosario	[A.25]	PR-MB				B	
Teléfonos IP - San José	[N.*]	PR-MB				B	
Teléfonos IP - San José	[I.1]	PR-MB				B	
Teléfonos IP - San José	[I.2]	PR-MB				B	
Teléfonos IP - San José	[A.25]	PR-MB				B	
Teléfonos IP - Ingenio	[N.*]	PR-MB				B	
Teléfonos IP - Ingenio	[I.1]	PR-MB				B	
Teléfonos IP - Ingenio	[I.2]	PR-MB				B	
Teléfonos IP - Ingenio	[A.25]	PR-MB				B	
Lectores de tarjetas de proximidad - El Rosario	[N.*]	PR-MB				A	
Lectores de tarjetas de proximidad - El Rosario	[I.1]	PR-MB				A	
Lectores de tarjetas de proximidad - El Rosario	[I.2]	PR-B				MA	
Lectores de tarjetas de proximidad - El Rosario	[I.6]	PR-M				MA	

Lectores de tarjetas de proximidad - El Rosario	[A.23]	PR-MB				A	
Lectores de tarjetas de proximidad - El Rosario	[A.25]	PR-MB				A	
Lectores de tarjetas de proximidad - San José	[N.*]	PR-MB				A	
Lectores de tarjetas de proximidad - San José	[I.1]	PR-MB				A	
Lectores de tarjetas de proximidad - San José	[I.2]	PR-B				MA	
Lectores de tarjetas de proximidad - San José	[I.6]	PR-M				MA	
Lectores de tarjetas de proximidad - San José	[A.23]	PR-MB				A	
Lectores de tarjetas de proximidad - San José	[A.25]	PR-MB				A	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[N.*]	PR-MB				A	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.1]	PR-MB				A	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.2]	PR-B				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[I.6]	PR-M				MA	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[A.23]	PR-MB				A	
Lectores de tarjetas de proximidad - El Ingenio (Aulas, Biblioteca, Administrativo)	[A.25]	PR-MB				A	
Servidores - El Rosario	[N.*]	PR-MB				A	
Servidores - El Rosario	[I.6]	PR-M				MA	
Servidores - El Rosario	[I.7]	PR-B				MA	
Servidores - El Rosario	[E.2]	PR-MB				A	
Servidores - El Rosario	[E.23]	PR-MB	A			A	M

Servidores - El Rosario	[A.6]	PR-MB				A	M
NAS - El Rosario	[N.*]	PR-MB				B	
NAS - El Rosario	[I.6]	PR-M				M	
NAS - El Rosario	[I.7]	PR-B				M	
NAS - El Rosario	[E.2]	PR-MB				B	
NAS - El Rosario	[E.23]	PR-MB	B			B	MB
NAS - El Rosario	[A.6]	PR-MB				B	MB
Ofimática - Toda la Institución	[E.20]	PR-MB		B	B	B	
Ofimática - Toda la Institución	[E.21]	PR-B				M	B
Sistema Operativo Cliente - Toda la Institución	[E.20]	PR-MB		B	B	B	
Sistema Operativo Cliente - Toda la Institución	[E.21]	PR-B				M	B
Sistema Operativo Cliente - Toda la Institución	[A.11]	PR-MB	B	B	B	B	B
Motor de Base de Datos - Servicios de Gestión Académica.	[E.20]	PR-MB		A	A	A	
Motor de Base de Datos - Servicios de Gestión Académica.	[E.21]	PR-B				MA	MA
Motor de Base de Datos - Servicios de Gestión Académica.	[A.6]	PR-MB	A	A	A	A	A
Motor de Base de Datos - Servicios de Gestión Académica.	[A.11]	PR-MB	A	A	A	A	A
Sistema Operativo Servidores - Toda la Institución	[E.20]	PR-MB		M	M	M	
Sistema Operativo Servidores - Toda la Institución	[E.21]	PR-B				A	M
Sistema Operativo Servidores - Toda la Institución	[A.6]	PR-MB	M	M	M	M	M
Sistema Operativo Servidores - Toda la Institución	[A.11]	PR-MB	M	M	M	M	M
Licencia de Escritorio Remoto - Dispositivo - Servicios de Gestión Académica.	[A.25]	PR-MB				M	
Aplicaciones de Desarrollo - Servicios de Gestión Académica.	[A.25]	PR-MB				M	
Servidor de Terminal Services - Servicios de Gestión Académica.	[E.20]	PR-MB	M	M	M	M	MB

Servidor de Terminal Services - Servicios de Gestión Académica.	[E.21]	PR-B				A	M
Servidor de Terminal Services - Servicios de Gestión Académica.	[A.6]	PR-MB	M	M	M	M	M
Servidor de Terminal Services - Servicios de Gestión Académica.	[A.11]	PR-MB	M	M	M	M	M
Servidor de Terminal Services - Servicios de Gestión Académica.	[E.2]	PR-MB	M	M	M	M	M
Servidor Directorio Activo - Toda la Institución	[E.20]	PR-MB	A	A	A	A	M
Servidor Directorio Activo - Toda la Institución	[E.21]	PR-B				MA	MA
Servidor Directorio Activo - Toda la Institución	[A.6]	PR-MB	A	A	A	A	A
Servidor Directorio Activo - Toda la Institución	[A.11]	PR-MB	A	A	A	A	A
Servidor Directorio Activo - Toda la Institución	[E.2]	PR-MB	A	A	A	A	A
Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.20]	PR-MB	A	A	A	A	M
Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.21]	PR-B				MA	A
Servidor de Aplicaciones - Servicios de Gestión Académica.	[A.6]	PR-MB	A	A	A	A	A
Servidor de Aplicaciones - Servicios de Gestión Académica.	[A.11]	PR-MB	A	A	A	A	A
Servidor de Aplicaciones - Servicios de Gestión Académica.	[E.2]	PR-MB	A	A	A	A	A
Licencia de Antivirus Clientes - Toda la Institución	[A.25]	PR-MB				M	MB
Servidor DHCP - Toda la Institución	[E.20]	PR-MB	A			A	B
Servidor DHCP - Toda la Institución	[E.21]	PR-B				MA	A
Servidor DHCP - Toda la Institución	[A.6]	PR-MB	A			A	A
Servidor DHCP - Toda la Institución	[A.11]	PR-MB	A			A	A
Servidor DHCP - Toda la Institución	[E.2]	PR-MB	A			A	A
Servidor Antivirus - Toda la Institución	[E.20]	PR-MB	M			M	MB

Servidor Antivirus - Toda la Institución	[E.21]	PR-B				A	M
Servidor Antivirus - Toda la Institución	[A.6]	PR-MB	M			M	M
Servidor Antivirus - Toda la Institución	[A.11]	PR-MB	M			M	M
Servidor Antivirus - Toda la Institución	[E.2]	PR-MB	M			M	M
Servidor de Backup MV - Toda la Institución	[E.20]	PR-MB	A	A	A	A	B
Servidor de Backup MV - Toda la Institución	[E.21]	PR-B				MA	A
Servidor de Backup MV - Toda la Institución	[A.6]	PR-MB	A	A	A	A	A
Servidor de Backup MV - Toda la Institución	[A.11]	PR-MB	A	A	A	A	A
Servidor de Backup MV - Toda la Institución	[E.2]	PR-MB	A	A	A	A	A
Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.20]	PR-MB	A	A	A	A	M
Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.21]	PR-B				MA	MA
Servidor de Backup Archivos - Servicios de Gestión Académica.	[A.6]	PR-MB	A	A	A	A	A
Servidor de Backup Archivos - Servicios de Gestión Académica.	[A.11]	PR-MB	A	A	A	A	A
Servidor de Backup Archivos - Servicios de Gestión Académica.	[E.2]	PR-MB	A	A	A	A	A
Base de Datos Estudiantes - Servicios de Gestión Académica.	[E.1]	PR-B		MA	MA	MA	MA
Base de Datos Estudiantes - Servicios de Gestión Académica.	[E.15]	PR-B		A	MA	MA	MA
Base de Datos Estudiantes - Servicios de Gestión Académica.	[A.11]	PR-MB	A	A	A	A	A
Base de Datos Docentes - Servicios de Gestión Académica.	[E.1]	PR-B		MA	MA	MA	MA
Base de Datos Docentes - Servicios de Gestión Académica.	[E.15]	PR-B		A	MA	MA	MA

Base de Datos Docentes - Servicios de Gestión Académica.	[A.11]	PR-MB	A	A	A	A	A
Base de Datos Personal Administrativo - Toda la Institución	[E.1]	PR-B		MA	MA	MA	MA
Base de Datos Personal Administrativo - Toda la Institución	[E.15]	PR-B		A	MA	MA	MA
Base de Datos Personal Administrativo - Toda la Institución	[A.11]	PR-MB	A	A	A	A	A
Estudiantes - Toda la Institución	[A.5]	PR-MB		A			
Estudiantes - Toda la Institución	[E.28]	PR-MB				A	
Docentes - Toda la Institución	[A.5]	PR-MB	A	A	A	A	
Docentes - Toda la Institución	[E.28]	PR-MB				A	
Personal Administrativo - Toda la Institución	[E.28]	PR-MB				M	
Personal Administrativo - Toda la Institución	[A.28]	PR-MB				M	
Personal Administrativo - Toda la Institución	[A.30]	PR-MB		M			M
Administrador de Infraestructura - Toda la Institución	[E.28]	PR-MB				A	
Administrador de Infraestructura - Toda la Institución	[A.28]	PR-MB				A	
Administrador de Infraestructura - Toda la Institución	[A.30]	PR-MB		A			A
Administrador Base de Datos - Toda la Institución	[E.28]	PR-MB				A	
Administrador Base de Datos - Toda la Institución	[A.28]	PR-MB				A	
Administrador Base de Datos - Toda la Institución	[A.30]	PR-MB		A			A
Correo Electrónico - Google Suite	[I.8]	PR-MB				M	
Correo Electrónico - Google Suite	[E.2]	PR-MB	B	M	M	M	M
Correo Electrónico - Google Suite	[A.24]	PR-MB				M	
Herramienta Colaborativa - Google Suite	[I.8]	PR-MB				B	
Herramienta Colaborativa - Google Suite	[E.2]	PR-MB	MB	B	B	B	B

Herramienta Colaborativa - Google Suite	[A.24]	PR-MB				B	
IaaS - CNT	[I.8]	PR-MB				A	
IaaS - CNT	[E.2]	PR-MB	A	A	A	A	A
IaaS - CNT	[A.24]	PR-MB				A	
Sistema Académico - Power Campus - Front End	[I.8]	PR-MB				A	
Sistema Académico - Power Campus - Front End	[E.1]	PR-MB	A	A	A	A	A
Sistema Académico - Power Campus - Front End	[A.24]	PR-MB				A	
Sistema Académico - Power Campus - Back End	[I.8]	PR-MB				A	
Sistema Académico - Power Campus - Back End	[E.2]	PR-MB	A	A	A	A	A
Sistema Académico - Power Campus - Back End	[A.24]	PR-MB				A	
Sistema Virtual de Aprendizaje - D2L -Front End	[I.8]	PR-MB				A	
Sistema Virtual de Aprendizaje - D2L -Front End	[E.1]	PR-MB	A	A	A	M	A
Sistema Virtual de Aprendizaje - D2L -Front End	[A.24]	PR-MB				A	
Sistema Virtual de Aprendizaje - D2L - Back End	[I.8]	PR-MB				A	
Sistema Virtual de Aprendizaje - D2L - Back End	[E.2]	PR-MB	A	A	A	A	A
Sistema Virtual de Aprendizaje - D2L - Back End	[A.24]	PR-MB				A	
Usuario Externo -	[E.28]	PR-MB				A	
Usuario Interno -	[E.28]	PR-MB				A	

ANEXO III

NIVEL DE CUMPLIMIENTO DE LA ISO 27002:2013 BASADO EN EL ANÁLISIS DE LOS 114 CONTROLES.

	%cumplimiento		
Control	**Actual**	**Después**	**Proyecto**
5 POLITICAS DE SEGURIDAD	**20%**	**80%**	Implantación de políticas de seguridad de la información.
5.1 Directrices de la Dirección en seguridad de la información	20%	80%	
5.1.1 Conjunto de políticas para la seguridad de la información	20%	80%	
5.1.2 Revisión de la Política de Seguridad de la Información	20%	80%	
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	**4%**	**80%**	Implantación de políticas de seguridad de la información.
6.1 Organización Interna	8%	80%	
6.1.1 Asignación de Responsabilidades para la Seguridad de la Información	0%	80%	
6.1.2 Segregación de tareas.	20%	80%	
6.1.3 Contacto con la Autoridades	20%	80%	
6.1.4 Contacto con Grupos de Interés Especial	0%	80%	
6.1.5 Seguridad de la información en la gestión de proyectos.	0%	80%	
6.2 Dispositivos para movilidad y teletrabajo.	0%	0%	
6.2.1 Política de uso de dispositivos para movilidad.	0%	0%	NO APLICA
6.2.2 Teletrabajo.	0%	0%	NO APLICA
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**25%**	**61%**	Implantación de políticas de seguridad de la información.
7.1 Antes de la contratación	35%	70%	Mejora en la gestión de Recursos Humanos

7.1.1 Investigación de Antecedentes	30%	60%	
7.1.2 Términos y condiciones de Contratación	40%	80%	
7.2 Durante la contratación	20%	63%	Plan de formación y concientización
7.2.1 Responsabilidad de la gestión	40%	60%	
7.2.2 Concienciación. Formación y capacitación en seguridad de la información	10%	80%	
7.2.3 Procesos Disciplinario	10%	50%	
7.3 Cese o Cambio de Puesto de Trabajo	20%	50%	
7.3.1 Cese o Cambio de Puesto de Trabajo	20%	50%	
8 GESTION DE ACTIVOS	**23%**	**58%**	Implantación de políticas de seguridad de la información.
8.1 Responsabilidad Sobre Los Activos	60%	68%	
8.1.1 Inventario de Activos	90%	90%	
8.1.2 Propiedad de los Activos	50%	50%	Mejora en la gestión de Recursos Humanos
8.1.3 Uso aceptable de los Activos	50%	80%	
8.1.4 Devolución de activos	50%	50%	
8.2 Clasificación de la Información	10%	57%	Clasificación de la Información
8.2.1 Directrices de Clasificación	0%	60%	
8.2.2 Etiquetado y manipulación de la Información	30%	60%	
8.2.3 Manipulación de activos	0%	50%	
8.3 Manejo de los soportes de almacenamiento.	0%	50%	
8.3.1 Gestión de soportes extraíbles.	0%	50%	
8.3.2 Eliminación de soportes.	0%	50%	
8.3.3 Soportes físicos en tránsito.	0%	50%	
9 CONTROL DE ACCESO	**40%**	**78%**	Implantación de políticas de seguridad de la información.

9.1 Requisitos de Negocio para el Control de Acceso	55%	85%	Políticas de control de acceso a la red y servicios de red
9.1.1 Política de Control de Acceso	30%	80%	Clasificación de la Información
9.1.2 Control de acceso a las redes y servicios asociados	80%	90%	Migración de dispositivos de seguridad de red (firewall/IDS/IPS).
9.2 Gestión de Acceso de Usuarios	23%	80%	Gestión del acceso del usuario
9.2.1 Gestión de altas/bajas en el registro de usuarios.	60%	80%	
9.2.2 Gestión de los derechos de acceso asignados a usuarios	20%	80%	
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	0%	80%	
9.2.4 Gestión de información confidencial de autenticación de usuarios.	40%	80%	
9.2.5 Revisión de los derechos de acceso de los usuarios.	0%	80%	
9.2.6 Retirada o adaptación de los derechos de acceso	20%	80%	
9.3 Responsabilidades de los Usuarios	20%	80%	
9.3.1 Uso de información confidencial para la autenticación	20%	80%	
9.4 Control de acceso a sistemas y aplicaciones.	62%	68%	
9.4.1 Restricción del acceso a la información.	40%	60%	Control de acceso al sistema y aplicaciones
9.4.2 Procedimientos seguros de inicio de sesión.	80%	80%	Control de acceso al sistema y aplicaciones
9.4.3 Gestión de contraseñas	80%	80%	Control de acceso al sistema y aplicaciones
9.4.4 Uso de herramientas de administración de sistemas	60%	70%	Instalación de un sistema de respaldos y recuperación.
9.4.5 Control de acceso al código fuente de los programas	50%	50%	Control de acceso al sistema y aplicaciones

10 CIFRADO	**0%**	**60%**	Implantación de políticas de seguridad de la información.
10.1 Controles criptográficos	0%	60%	Migración de dispositivos de seguridad de red (firewall/IDS/IPS).
10.1.1 Política de uso de los controles criptográficos	0%	80%	
10.1.2 Gestión de claves	0%	40%	
11 SEGURIDAD FISICA Y AMBIENTAL	**60%**	**77%**	Implantación de políticas de seguridad de la información.
11.1 Áreas Seguras	88%	88%	Repotenciar Data Center.
11.1.1 Perímetro de Seguridad Física	100%	100%	
11.1.2 Controles Físicos de Entrada	100%	100%	
11.1.3 Seguridad de Oficinas, despachos e instalaciones	100%	100%	
11.1.4 Protección contra las amenazas externas y de origen ambiental	90%	90%	
11.1.5 Trabajo en Áreas seguras	90%	90%	
11.1.6 Áreas de acceso público, carga y descarga	50%	50%	
11.2 Seguridad de los Equipos	32%	66%	
11.2.1 Emplazamiento y protección de los equipos	60%	65%	Migración de dispositivos de seguridad de red (firewall/IDS/IPS).
11.2.2 Instalaciones de suministros	60%	60%	
11.2.3 Seguridad del Cableado	80%	80%	
11.2.4 Mantenimiento de los Equipos	90%	90%	
11.2.5 Salida de activos fuera de las dependencias de la empresa.	0%	60%	
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	0%	60%	
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	0%	0%	
11.2.8 Equipo informático de usuario desatendido	0%	80%	

11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	0%	100%	
12 SEGURIDAD EN LA OPERATIVA.	**49%**	**64%**	Implantación de políticas de seguridad de la información.
12.1 Responsabilidades y Procedimientos de Operación	25%	26%	
12.1.1 Documentación de los Procedimientos de Operación	40%	45%	
12.1.2 Gestión de Cambios	0%	0%	
12.1.3 Gestión de capacidades.	0%	0%	
12.1.4 Separación de entornos de desarrollo, prueba y producción.	60%	60%	
12.2 Protección contra Código Malicioso	60%	65%	
12.2.1 Controles contra el código malicioso	60%	65%	Migración de dispositivos de seguridad de red (firewall/IDS/IPS).
12.3 Copias de Seguridad	60%	80%	
12.3.1 Copias de Seguridad de la Información	60%	80%	Instalación de un sistema de respaldos y recuperación.
12.4 Registro de actividad y supervisión.	68%	69%	Migración de dispositivos de seguridad de red (firewall/IDS/IPS).
12.4.1 Registro y gestión de eventos de actividad.	60%	65%	Repotenciar Data Center.
12.4.2 Protección de los registros Información	60%	60%	
12.4.3 Registros de actividad del administrador y operador del sistema.	60%	60%	
12.4.4 Sincronización del Reloj	90%	90%	
12.5 Control del software en explotación.	90%	90%	
12.5.1 Instalación del software en sistemas en producción.	90%	90%	
12.6 Gestión de la vulnerabilidad técnica	30%	60%	Migración de dispositivos de seguridad de red (firewall/IDS/IPS).
12.6.1 Gestión de las vulnerabilidades técnicas.	40%	60%	

12.6.2 Restricciones en la instalación de software	20%	60%	
12.7 Consideraciones de las auditorías de los sistemas de información	10%	60%	Control de acceso al sistema y aplicaciones
12.7.1 Controles de auditoría de los sistemas de información.	10%	60%	
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	**44%**	**52%**	Migración de dispositivos de seguridad de red (firewall/IDS/IPS).
13.1 Gestión de Seguridad de las Redes	83%	83%	Repotenciar Data Center.
13.1.1 Controles de Red	90%	90%	
13.1.2 Mecanismos de seguridad asociados a servicios en red.	80%	80%	
13.1.3 Intercambio de información con partes externas Segregación de redes.	80%	80%	
13.2 Intercambio de información con partes externas	5%	20%	
13.2.1 Políticas y Procedimientos de Intercambio de Información	0%	0%	
13.2.2 Acuerdo de Intercambio	0%	0%	
13.2.3 Mensajería Electrónica	0%	0%	
13.2.4 Acuerdos de confidencialidad y secreto.	20%	80%	Mejora en la gestión de Recursos Humanos
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	**29%**	**36%**	Migración de dispositivos de seguridad de red (firewall/IDS/IPS).
14.1 Requisitos de Seguridad de los Sistemas de Información	67%	67%	
14.1.1 Análisis y especificaciones de los requisitos de seguridad	40%	40%	
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	80%	80%	
14.1.3 Protección de las transacciones por redes telemáticas.	80%	80%	

14.2 Seguridad en los procesos de Desarrollo y Soporte	20%	40%	Implantación de políticas de seguridad de la información.
14.2.1 Política de desarrollo seguro de software.	0%	100%	
14.2.2 Procedimientos de control de cambios en los sistemas	0%	80%	
14.2.3 Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo	0%	0%	
14.2.4 Restricciones a los cambios en los paquetes de software	0%	0%	
14.2.5 Uso de principios de ingeniería en protección de sistemas.	20%	20%	
14.2.6 Seguridad en entornos de desarrollo.	0%	0%	
14.2.7 Externalización del Desarrollo del software	0%	0%	
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	80%	80%	
14.2.9 Pruebas de aceptación.	80%	80%	
14.3 Datos de prueba	0%	0%	
14.3.1 Protección de los datos utilizados en pruebas.	0%	0%	
15 RELACIONES CON SUMINISTRADORES.	**40%**	**40%**	
15.1 Seguridad de la información en las relaciones con suministradores	0%	0%	
15.1.1 Política de seguridad de la información para suministradores	0%	0%	
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	0%	0%	
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	0%	0%	
15.2 Gestión de la prestación del servicio por suministradores.	80%	80%	

15.2.1 Supervisión y revisión de los servicios prestados por terceros.	80%	80%	
15.2.2 Gestión de cambios en los servicios prestados por terceros.	80%	80%	
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	**0%**	**100%**	Implementar un CSIRT
16.1 Gestión de Incidentes de Seguridad de la Información y Mejoras	0%	100%	
16.1.1 Responsabilidades y Procedimientos	0%	100%	
16.1.2 Notificación de los Eventos de Seguridad de la Información	0%	100%	
16.1.3 Notificación de Puntos Débiles de la Seguridad	0%	100%	
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	0%	100%	
16.1.5 Respuesta a los incidentes de seguridad.	0%	100%	
16.1.6 Aprendizaje de los Incidentes de Seguridad de la Información	0%	100%	
16.1.7 Recopilación de Evidencias	0%	100%	
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**40%**	**58%**	Instalación de un sistema de respaldos y recuperación.
17.1 Continuidad de la seguridad de la información	0%	27%	Migración de dispositivos de seguridad de red (firewall/IDS/IPS).
17.1.1 Planificación de la continuidad de la seguridad de la información	0%	20%	Repotenciar Data Center.
17.1.2 Implantación de la continuidad de la seguridad de la información	0%	60%	
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	0%	0%	
17.2 Redundancias	80%	90%	Repotenciar Data Center.

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	80%	90%	
18 CUMPLIMIENTO	**12%**	**42%**	Implantación de políticas de seguridad de la información.
18.1 Cumplimiento de los requisitos legales y contractuales	24%	58%	
18.1.1 Identificación de la legislación aplicable	80%	80%	
18.1.2 Derechos de Propiedad Intelectual (DPI)	0%	80%	Mejora en la gestión de Recursos Humanos
18.1.3 Protección de los registros de la Organización	20%	50%	
18.1.4 Protección de Datos y privacidad de la información personal	20%	80%	Mejora en la gestión de Recursos Humanos
18.1.5 Regulación de los Controles Criptográficos	0%	0%	
18.2 Revisiones de la seguridad de la información.	0%	27%	
18.2.1 Revisión independiente de la seguridad de la información.	0%	20%	
18.2.2 Cumplimiento de las políticas y normas de seguridad	0%	60%	
18.2.3 Comprobación del cumplimiento.	0%	0%	

ANEXO IV

PROYECTOS PLANTEADOS A LA DIRECCIÓN, DETALLANDO EL COSTE ECONÓMICO DE LOS MISMOS, SU PLANIFICACIÓN TEMPORAL Y SU IMPACTO SOBRE EL CUMPLIMIENTO NORMATIVO DE LA ISO/IEC 27002:2013 EN LOS DIFERENTES DOMINIOS.

Los proyectos planteados serán resultantes de agrupar un conjunto de recomendaciones identificadas en la fase de análisis de riesgos para facilitar su ejecución. Se incidirá no sólo en la mejora en relación con la gestión de la seguridad, sino también en posibles beneficios colaterales como puede ser la optimización de recursos, mejora en la gestión de procesos y tecnologías presentes en la organización analizada.

Los proyectos deben cuantificarse económicamente y planificarse en el tiempo, estableciendo plazos de consecución de sus objetivos (en general, corto, medio y largo plazo). Adicionalmente, deben incluirse en la planificación puntos de control que permitan considerar realmente el Plan de Implementación del SGSI como un proceso de mejora continua.

Es importante remarcar que los proyectos no deben limitarse al ámbito de la tecnología, sino que pueden (habitualmente, deben) afectar a los diferentes ámbitos (p.e. recursos humanos, organización), los proyectos que se aborden en estos aspectos deben también plantearse.

A continuación, se describe brevemente los proyectos planteados para minimizar el riesgo:

Código del proyecto: PRJ-001

Nombre del proyecto: Implantación de políticas de seguridad de la información.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-01
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%	35%
8 GESTION DE ACTIVOS	23%	30%
9 CONTROL DE ACCESO	40%	50%
10 CIFRADO	0%	60%
11 SEGURIDAD FISICA Y AMBIENTAL	60%	77%
12 SEGURIDAD EN LA OPERATIVA.	55%	60%
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	44%	44%
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%	0%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40%	40%
18 CUMPLIMIENTO	12%	20%

Cuadro 27: Impacto sobre el dominio de la seguridad PRJ-01

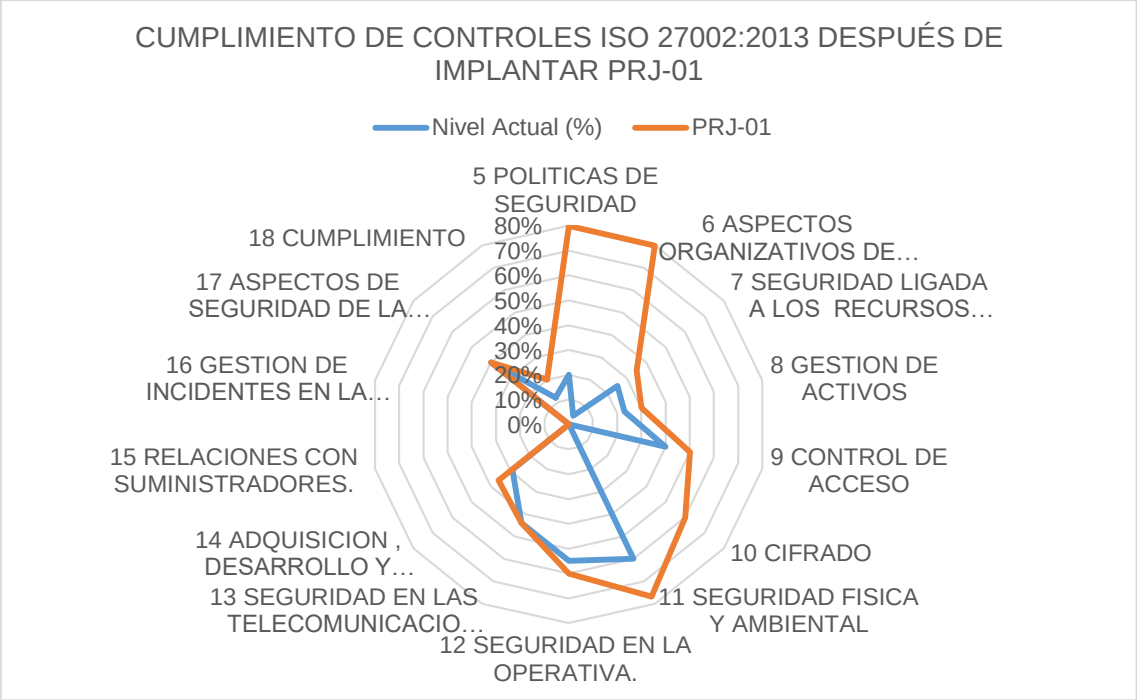

Gráfico 8: Cumplimiento de controles ISO 27002:2013 PRJ-01

Código del proyecto: PRJ-002

Nombre del proyecto: Instalación de un sistema de respaldos y recuperación.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-02
5 POLITICAS DE SEGURIDAD	**20%**	**20%**
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	**4%**	**4%**
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**25%**	**25%**
8 GESTION DE ACTIVOS	**23%**	**23%**

9 CONTROL DE ACCESO	**40%**	**45%**
10 CIFRADO	**0%**	**0%**
11 SEGURIDAD FISICA Y AMBIENTAL	**60%**	**60%**
12 SEGURIDAD EN LA OPERATIVA.	**55%**	**60%**
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	**44%**	**44%**
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	**29%**	**29%**
15 RELACIONES CON SUMINISTRADORES.	**40%**	**40%**
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	**0%**	**0%**
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**40%**	**50%**
18 CUMPLIMIENTO	**12%**	**12%**

Cuadro 28: Impacto sobre el dominio de la seguridad PRJ-02

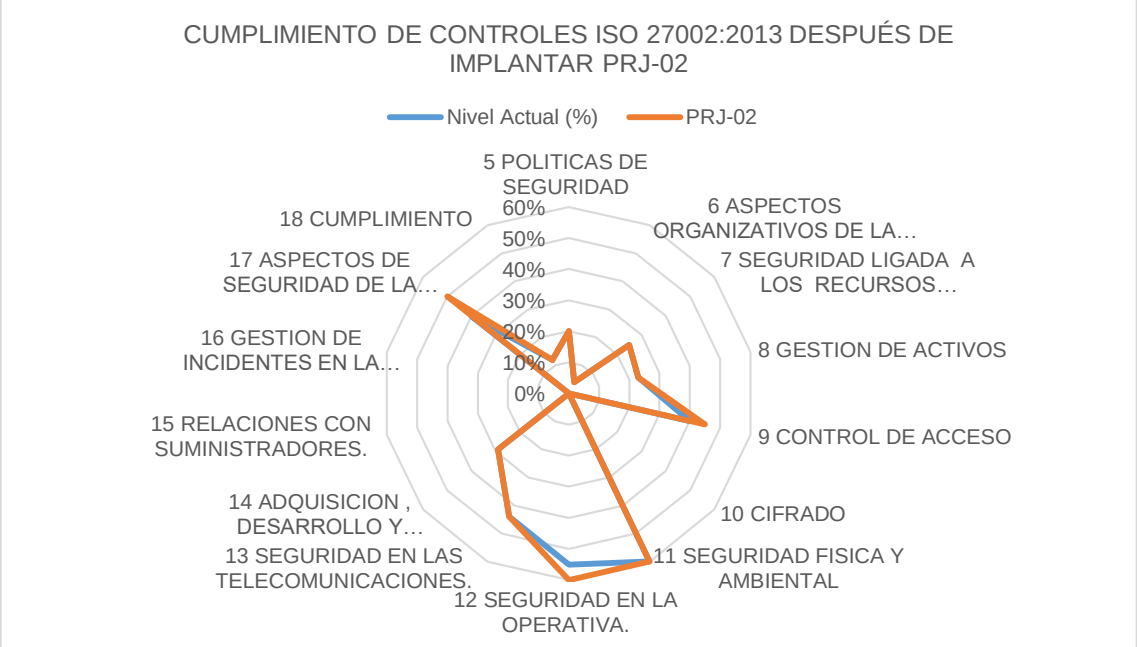

Gráfico 9: Cumplimiento de controles ISO 27002:2013 PRJ-02

Código del proyecto: PRJ-003

Nombre del proyecto: Migración de dispositivos de seguridad de red (firewall/IDS/IPS).

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-03
5 POLITICAS DE SEGURIDAD	20%	25%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	4%	25%
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	25%	25%
8 GESTION DE ACTIVOS	23%	23%
9 CONTROL DE ACCESO	40%	50%
10 CIFRADO	0%	10%
11 SEGURIDAD FISICA Y AMBIENTAL	60%	65%
12 SEGURIDAD EN LA OPERATIVA.	55%	64%
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	44%	48%
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	29%	30%
15 RELACIONES CON SUMINISTRADORES.	40%	40%
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	0%	0%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40%	50%
18 CUMPLIMIENTO	12%	12%

Cuadro 29: Impacto sobre el dominio de la seguridad PRJ-03

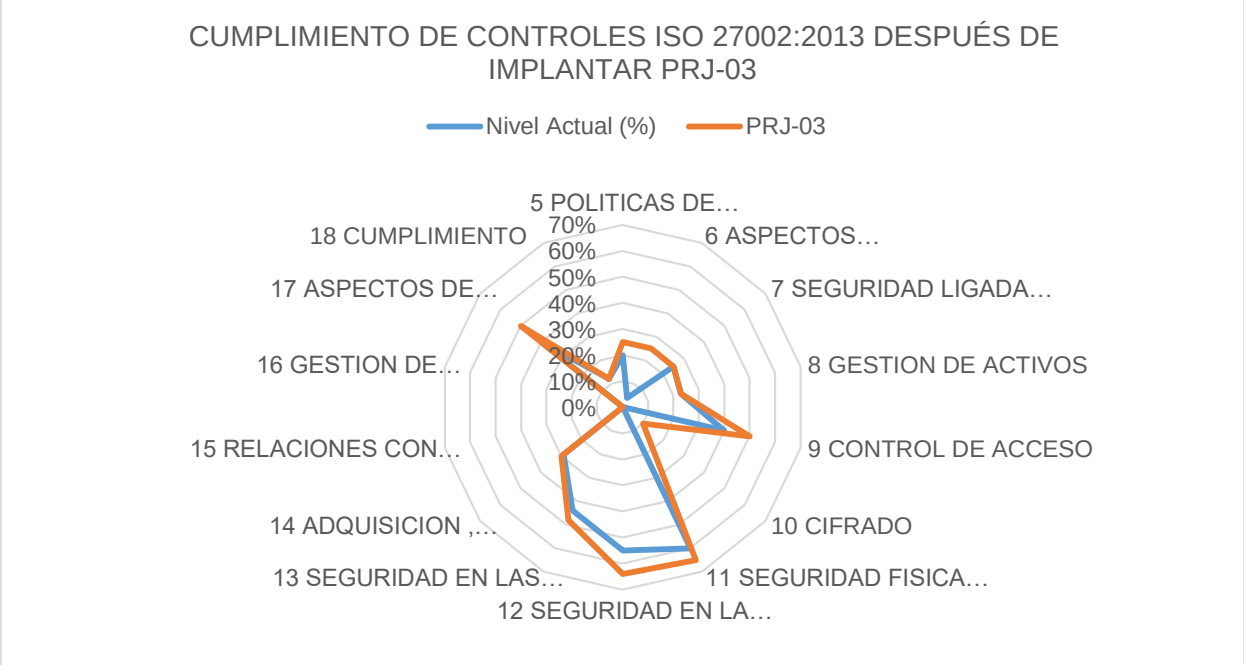

Gráfico 10: Cumplimiento de controles ISO 27002:2013 PRJ-03

Código del proyecto: PRJ-004

Nombre del proyecto: Repotenciar Data Center.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-04
5 POLITICAS DE SEGURIDAD	**20%**	**25%**
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	**4%**	**40%**
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**25%**	**25%**
8 GESTION DE ACTIVOS	**23%**	**23%**

9 CONTROL DE ACCESO	**40%**	**40%**
10 CIFRADO	**0%**	**0%**
11 SEGURIDAD FISICA Y AMBIENTAL	**60%**	**85%**
12 SEGURIDAD EN LA OPERATIVA.	**55%**	**55%**
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	**44%**	**44%**
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	**29%**	**29%**
15 RELACIONES CON SUMINISTRADORES.	**40%**	**40%**
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	**0%**	**0%**
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**40%**	**58%**
18 CUMPLIMIENTO	**12%**	**12%**

Cuadro 30: Impacto sobre el dominio de la seguridad PRJ-04

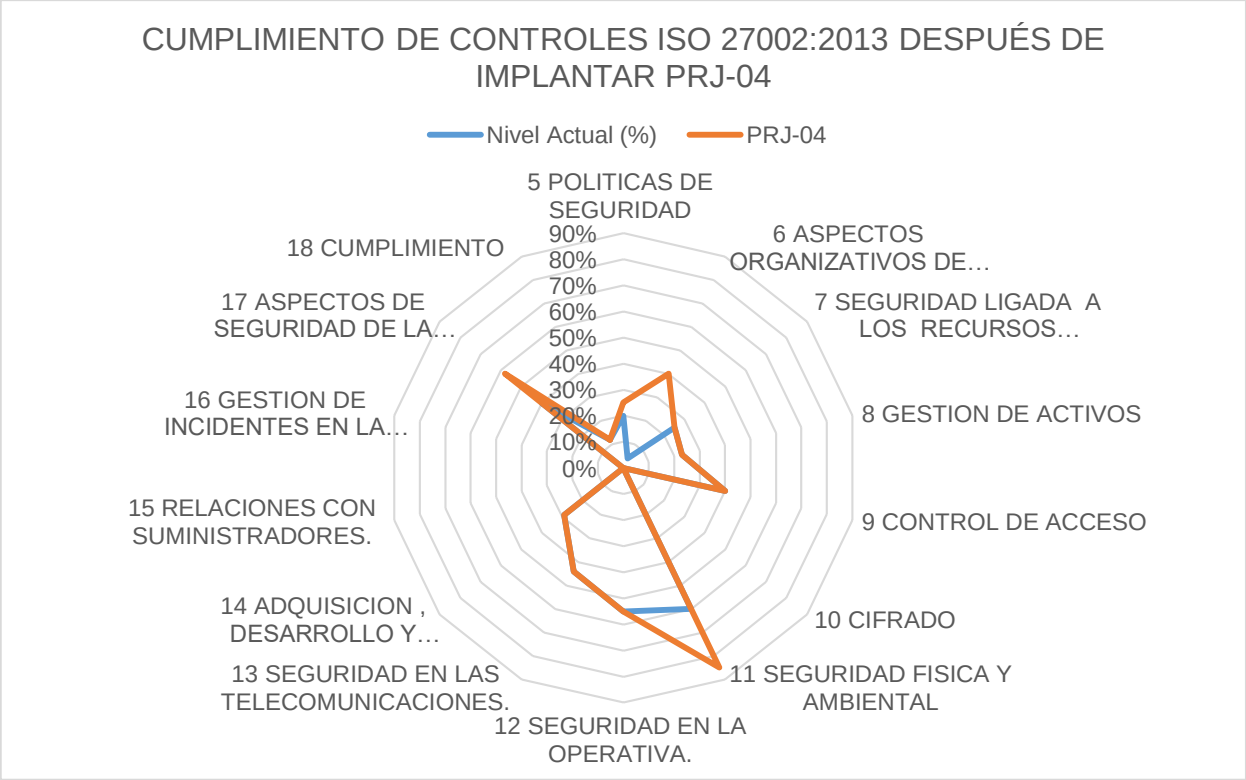

Gráfico 11: Cumplimiento de controles ISO 27002:2013 PRJ-04

Código del proyecto: PRJ-005

Nombre del proyecto: Plan de Formación y Concientización

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-04
5 POLITICAS DE SEGURIDAD	**20%**	**25%**
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	**4%**	**40%**
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**25%**	**25%**
8 GESTION DE ACTIVOS	**23%**	**23%**
9 CONTROL DE ACCESO	**40%**	**40%**
10 CIFRADO	**0%**	**0%**

11 SEGURIDAD FISICA Y AMBIENTAL	**60%**	**85%**
12 SEGURIDAD EN LA OPERATIVA.	**55%**	**55%**
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	**44%**	**44%**
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	**29%**	**29%**
15 RELACIONES CON SUMINISTRADORES.	**40%**	**40%**
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	**0%**	**0%**
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**40%**	**58%**
18 CUMPLIMIENTO	**12%**	**12%**

Cuadro 30: Impacto sobre el dominio de la seguridad PRJ-04

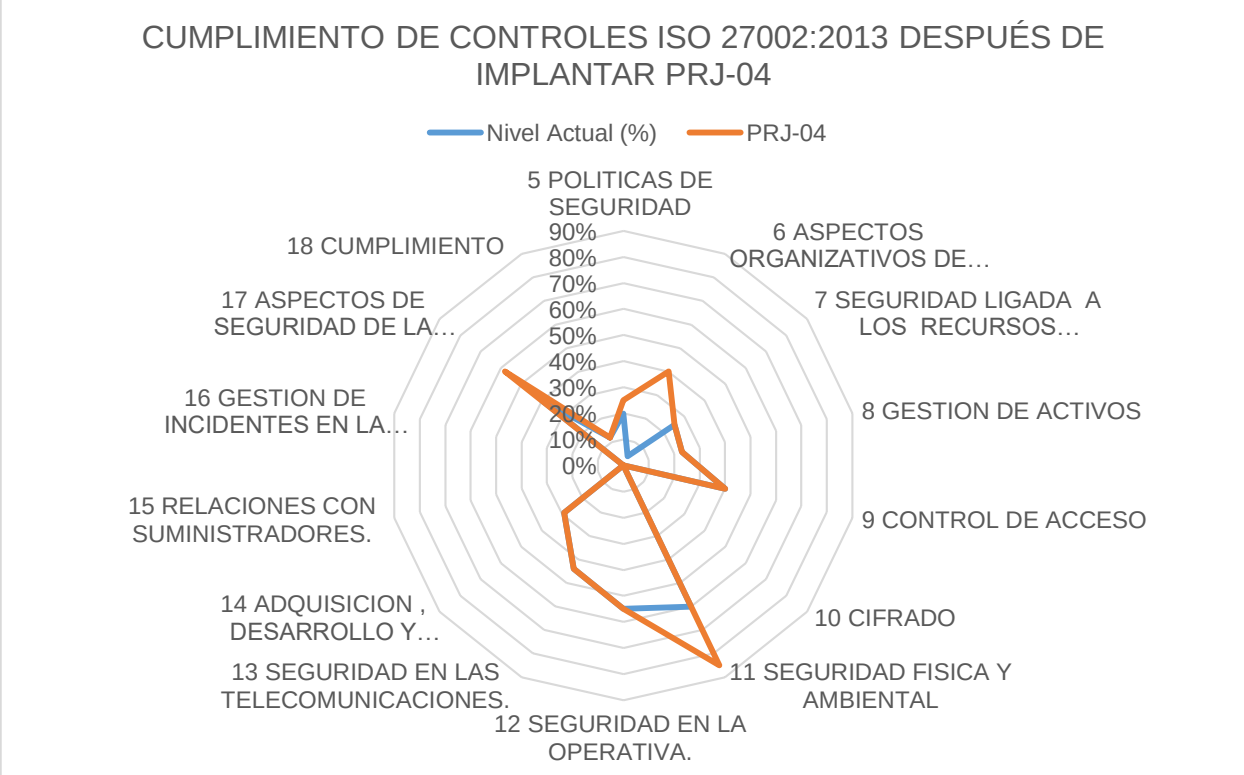

Gráfico 11: Cumplimiento de controles ISO 27002:2013 PRJ-04

Código del proyecto: PRJ-006

Nombre del proyecto: Políticas de control de acceso a la red y servicios de red.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-05
5 POLITICAS DE SEGURIDAD	20%	20%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	4%	4%
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	25%	63%
8 GESTION DE ACTIVOS	23%	23%
9 CONTROL DE ACCESO	40%	40%
10 CIFRADO	0%	0%
11 SEGURIDAD FISICA Y AMBIENTAL	60%	60%
12 SEGURIDAD EN LA OPERATIVA.	55%	55%
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	44%	44%
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	29%	29%
15 RELACIONES CON SUMINISTRADORES.	40%	40%
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	0%	0%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40%	40%
18 CUMPLIMIENTO	12%	12%

Cuadro 31: Impacto sobre el dominio de la seguridad PRJ-05

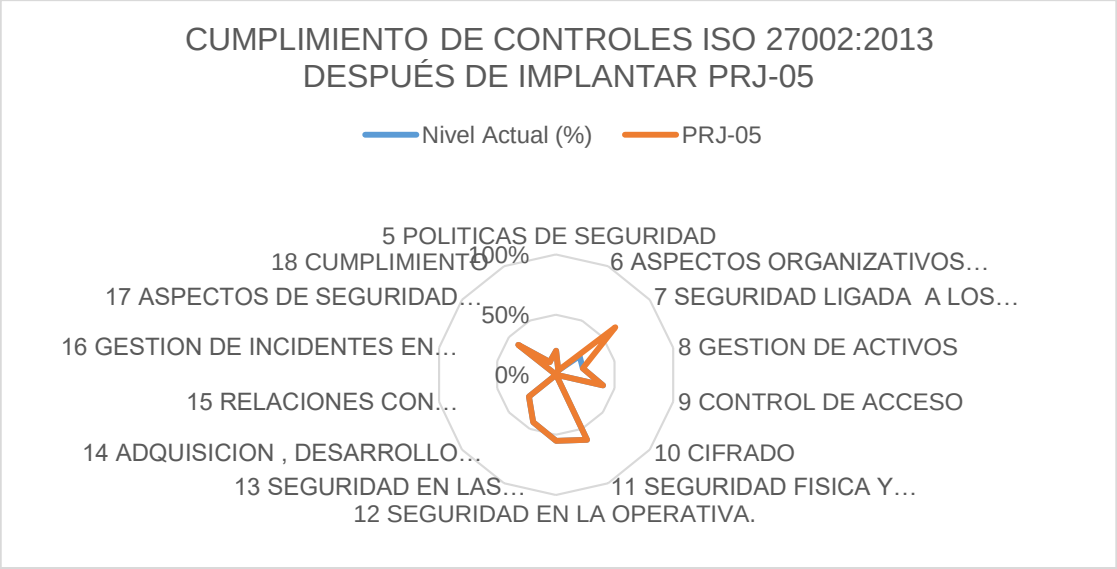

Gráfico 12: Cumplimiento de controles ISO 27002:2013 PRJ-05

Código del proyecto: PRJ-007

Nombre del proyecto: Control de acceso al sistema y aplicaciones.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-06
5 POLITICAS DE SEGURIDAD	**20%**	**20%**
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	**4%**	**4%**
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**25%**	**25%**
8 GESTION DE ACTIVOS	**23%**	**23%**
9 CONTROL DE ACCESO	**40%**	**60%**
10 CIFRADO	**0%**	**0%**
11 SEGURIDAD FISICA Y AMBIENTAL	**60%**	**60%**
12 SEGURIDAD EN LA OPERATIVA.	**55%**	**55%**
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	**44%**	**44%**

14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	**29%**	**29%**
15 RELACIONES CON SUMINISTRADORES.	**40%**	**40%**
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	**0%**	**0%**
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**40%**	**40%**
18 CUMPLIMIENTO	**12%**	**12%**

Cuadro 32: Impacto sobre el dominio de la seguridad PRJ-06

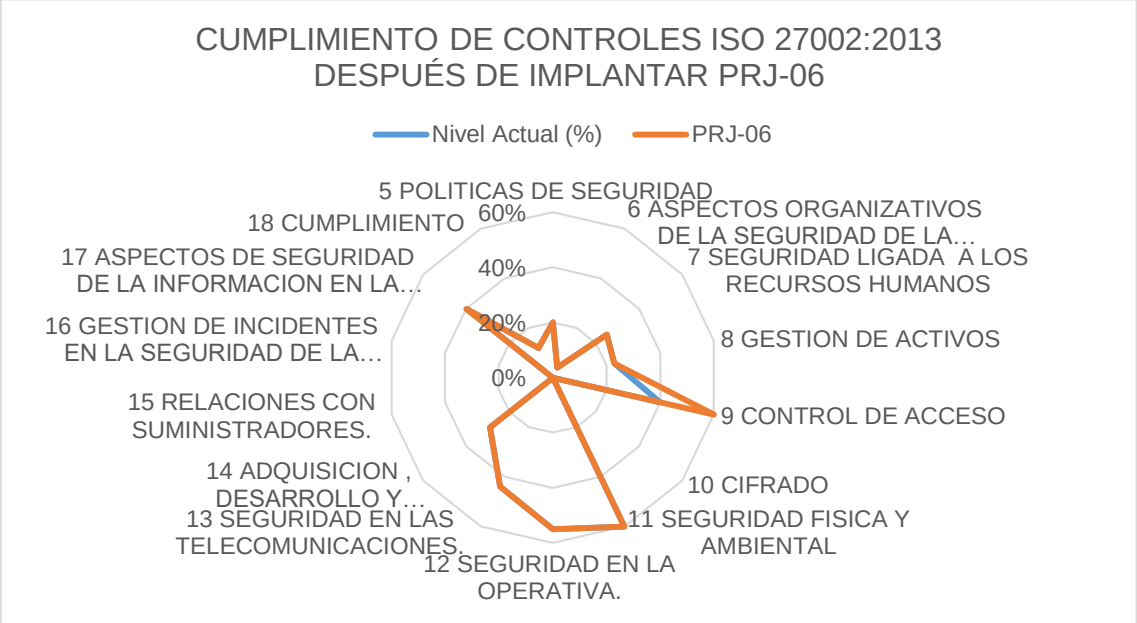

Gráfico 13: Cumplimiento de controles ISO 27002:2013 PRJ-06

Código del proyecto: PRJ-008

Nombre del proyecto: Control de acceso al sistema y aplicaciones.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-07
5 POLITICAS DE SEGURIDAD	20%	20%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	4%	4%
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	25%	25%
8 GESTION DE ACTIVOS	23%	23%
9 CONTROL DE ACCESO	40%	78%
10 CIFRADO	0%	0%
11 SEGURIDAD FISICA Y AMBIENTAL	60%	60%
12 SEGURIDAD EN LA OPERATIVA.	55%	55%
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	44%	44%
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	29%	29%
15 RELACIONES CON SUMINISTRADORES.	40%	40%
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	0%	0%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40%	40%
18 CUMPLIMIENTO	12%	12%

Cuadro 33: Impacto sobre el dominio de la seguridad PRJ-07

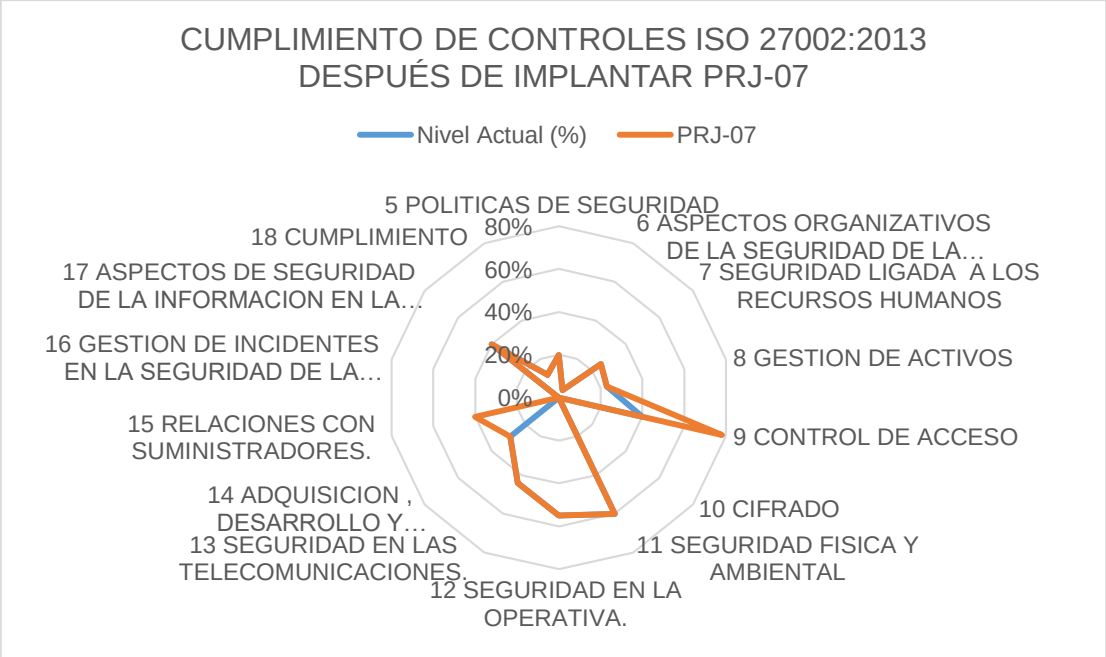

Gráfico 14: Cumplimiento de controles ISO 27002:2013 PRJ-07

Código del proyecto: PRJ-009

Nombre del proyecto: Mejora en la gestión de Recursos Humanos.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-08
5 POLITICAS DE SEGURIDAD	**20%**	**20%**
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	**4%**	**4%**
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**25%**	**25%**
8 GESTION DE ACTIVOS	**23%**	**23%**
9 CONTROL DE ACCESO	**40%**	**60%**
10 CIFRADO	**0%**	**0%**
11 SEGURIDAD FISICA Y AMBIENTAL	**60%**	**60%**
12 SEGURIDAD EN LA OPERATIVA.	**55%**	**64%**

13 SEGURIDAD EN LAS TELECOMUNICACIONES.	**44%**	**44%**
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	**29%**	**29%**
15 RELACIONES CON SUMINISTRADORES.	**40%**	**40%**
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	**0%**	**0%**
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**40%**	**40%**
18 CUMPLIMIENTO	**12%**	**12%**

Cuadro 34: Impacto sobre el dominio de la seguridad PRJ-08

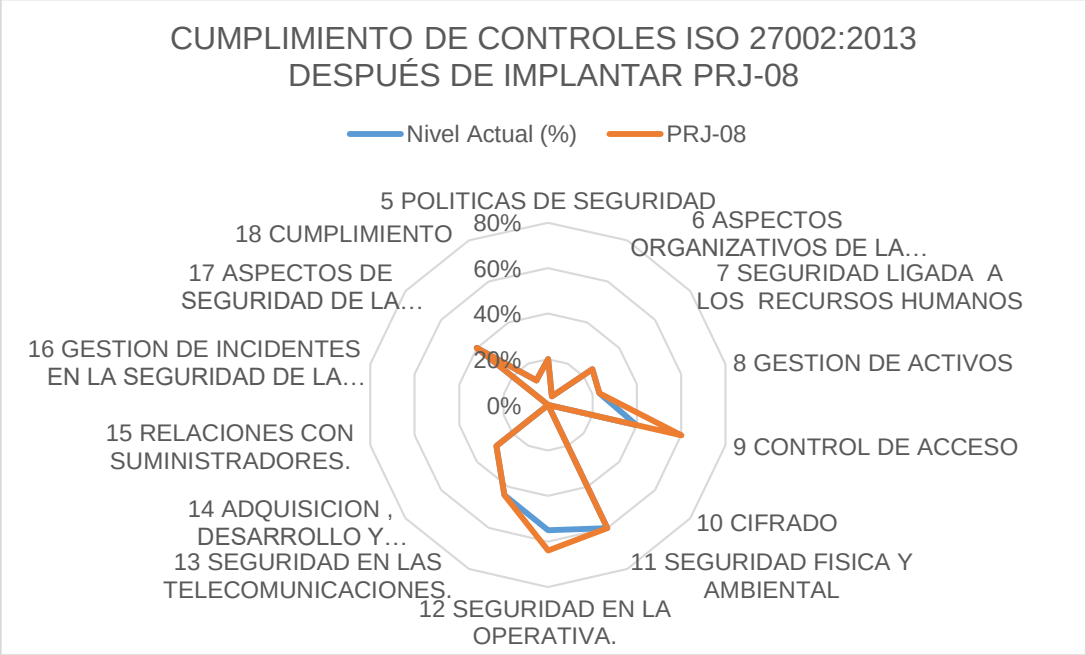

Gráfico 15: Cumplimiento de controles ISO 27002:2013 PRJ-08

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-09
5 POLITICAS DE SEGURIDAD	20%	20%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	4%	4%
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	25%	61%
8 GESTION DE ACTIVOS	23%	50%
9 CONTROL DE ACCESO	40%	40%
10 CIFRADO	0%	0%
11 SEGURIDAD FISICA Y AMBIENTAL	60%	60%
12 SEGURIDAD EN LA OPERATIVA.	55%	55%
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	44%	52%
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	29%	29%
15 RELACIONES CON SUMINISTRADORES.	40%	40%
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	0%	0%
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40%	40%
18 CUMPLIMIENTO	12%	42%

Cuadro 35: Impacto sobre el dominio de la seguridad PRJ-09

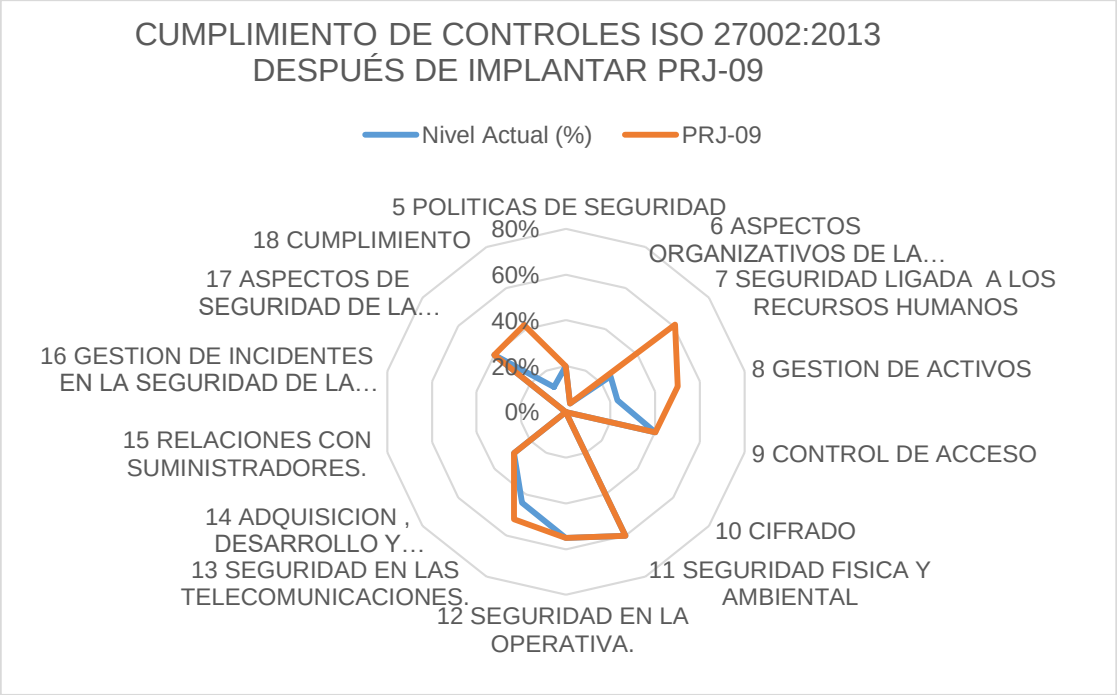

Gráfico 16: Cumplimiento de controles ISO 27002:2013 PRJ-09

Código del proyecto: PRJ-010

Nombre del proyecto: Clasificación de la Información.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-10
5 POLITICAS DE SEGURIDAD	**20%**	**20%**
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	**4%**	**4%**
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**25%**	**25%**
8 GESTION DE ACTIVOS	**23%**	**58%**
9 CONTROL DE ACCESO	**40%**	**70%**
10 CIFRADO	**0%**	**0%**
11 SEGURIDAD FISICA Y AMBIENTAL	**60%**	**60%**
12 SEGURIDAD EN LA OPERATIVA.	**55%**	**55%**

13 SEGURIDAD EN LAS TELECOMUNICACIONES.	**44%**	**44%**
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	**29%**	**29%**
15 RELACIONES CON SUMINISTRADORES.	**40%**	**40%**
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	**0%**	**0%**
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**40%**	**40%**
18 CUMPLIMIENTO	**12%**	**12%**

Cuadro 36: Impacto sobre el dominio de la seguridad PRJ-10

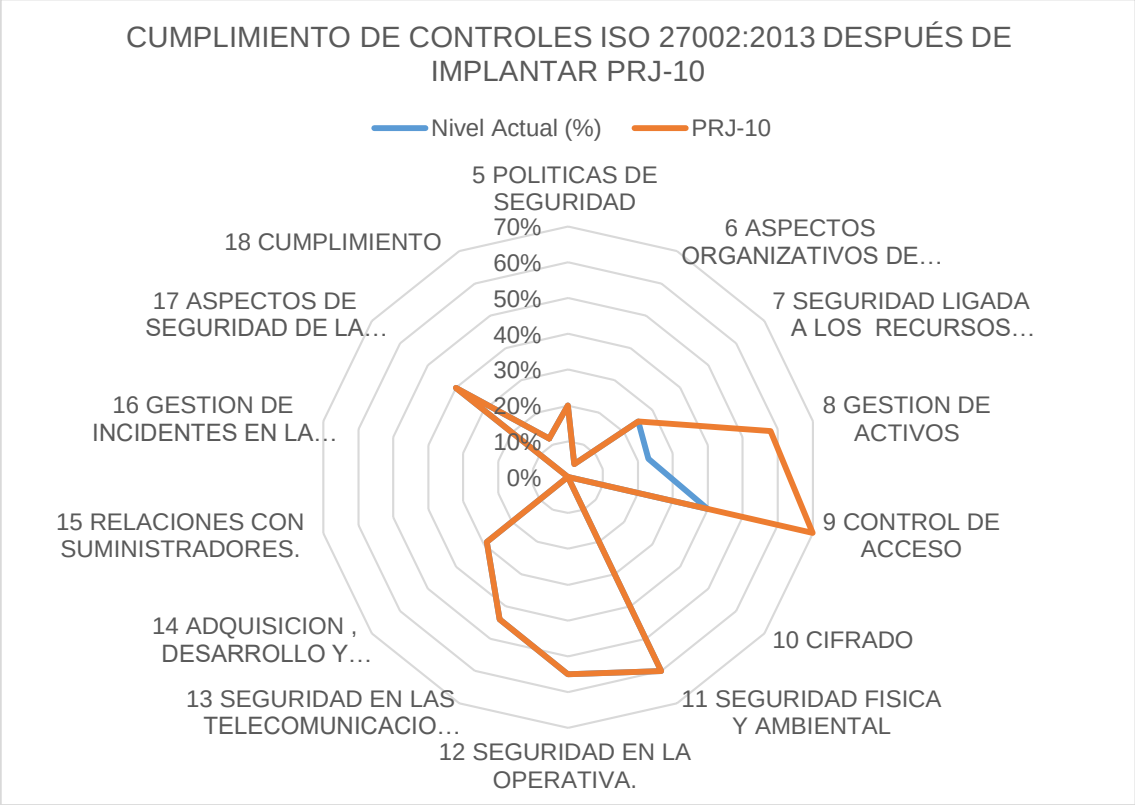

Gráfico 17: Cumplimiento de controles ISO 27002:2013 PRJ-10

Código del proyecto: PRJ-011

Nombre del proyecto: Implementar un CSIRT.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO

afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

CONTROL	Nivel Actual (%)	PRJ-11
5 POLITICAS DE SEGURIDAD	20%	20%
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	4%	4%
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	25%	25%
8 GESTION DE ACTIVOS	23%	23%
9 CONTROL DE ACCESO	40%	40%
10 CIFRADO	0%	0%
11 SEGURIDAD FISICA Y AMBIENTAL	60%	60%
12 SEGURIDAD EN LA OPERATIVA.	55%	55%
13 SEGURIDAD EN LAS TELECOMUNICACIONES.	44%	44%
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	29%	29%
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%	40%
18 CUMPLIMIENTO	12%	12%

Cuadro 37: Impacto sobre el dominio de la seguridad PRJ-11

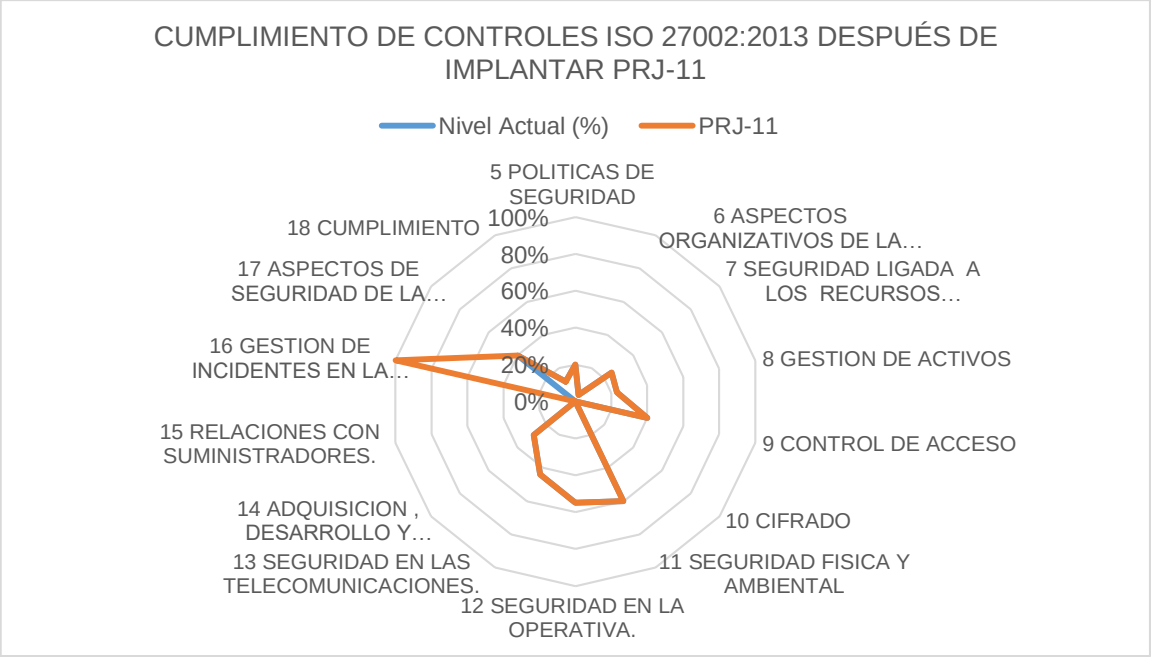

Gráfico 18: Cumplimiento de controles ISO 27002:2013 PRJ-11

En cuanto a la planificación temporal en la ejecución de los proyectos, tenemos lo siguiente:

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												

Cuadro 31: Plan de implementación de proyectos

ANEXO V

POLÍTICA DE SEGURIDAD

Políticas de Seguridad de la Información

Título de la Política	Política de Seguridad de la Información
Responsable	Edwin Pérez, Director de Técnologias de la Información y Comunicación,
Departamento	Dirección de TIC
Aprobado por	Comisión Gestora, aprobado en reunión del XX/XX/XXXX
Contacto	Luis Fernando Echeverría, Analista de TI
Fecha de Vigencia	Primera Versión: DD/MM/YYYY; revisión principal actual:
Última Actualización	

I. Declaración de Política

El propósito de esta política es proporcionar un marco de seguridad que garantice la protección de la información de la Universidad contra la pérdida, daño o el acceso no autorizado, al tiempo que apoya las necesidades de intercambio de información de nuestra cultura académica. La información de la Universidad puede ser verbal, digital y/o impresa, individualmente controlada o compartida, independiente o en red, utilizada para administración, investigación, enseñanza u otros propósitos. Las normas y procedimientos relacionados con esta Política de Seguridad de la Información se desarrollarán y publicarán por separado.

El incumplimiento de esta política puede someterle a acciones disciplinarias y a posibles sanciones descritas en el Estatuto de la Universidad.

II. Quién es afectado por esta política

La Política de Seguridad de la Información se aplica a todos los profesores y personal administrativo de la Universidad, así como a los estudiantes que actúan en nombre de la Universidad Yachay Tech, a través de servicios en los organismos de la Universidad tales como grupos de trabajo, consejos y comités (por ejemplo, el Comité de Profesores-Estudiantes sobre Disciplina). Esta política también se aplica a todas las demás personas y entidades a las que se concede el uso de la Información de la Universidad, incluyendo, pero no limitado a, contratistas, empleados temporales y pasantes.

III. Definiciones

Autorización - la función de establecer niveles de privilegio de un individuo para acceder y/o manejar información.
Disponibilidad - garantizar que la información esté lista y sea adecuada para su uso.
Confidencialidad - garantizar que la información se mantiene en estricta privacidad.
Integridad - garantizar la exactitud, integridad y consistencia de la información.
Acceso no autorizado - buscar, revisar, copiar, modificar, eliminar, analizar o manejar información sin la autorización adecuada y las necesidades legítimas del negocio.
Información de la Universidad - información que la Universidad de Yachay recoge, posee o tiene acceso a, independientemente de su fuente. Esto incluye información contenida en documentos impresos u otros medios, comunicados a través de redes de voz o datos, o intercambiados en conversación.

IV. Política

La Universidad de Yachay asegura apropiadamente su información de acceso no autorizado, pérdida o daño mientras apoya las necesidades, de intercambio de información de nuestra cultura académica.

A. Niveles de Clasificación

Toda la información de la Universidad se clasifica en uno de los cuatro niveles según su sensibilidad y los riesgos asociados con la divulgación. El nivel de clasificación determina las protecciones de seguridad que deben utilizarse para la información.

Al combinar información, el nivel de clasificación de la información resultante debe ser

reevaluado independientemente de la clasificación de la información de origen para gestionar los riesgos.

Los requisitos adicionales para la protección de la información en cada nivel de clasificación se identifican en las Normas y Procedimientos de Protección de Información de Yachay.

Los niveles de clasificación son:

1. Restringido

La siguiente información de la universidad está clasificada como Restringida:

- Número de seguridad social
- Número de cuenta bancaria
- Número de identificación del Estado
- Número de tarjeta de crédito
- Información de salud protegida (según lo definido por la Constitución, Ley de Salud Pública u otros) Que, de conformidad con el inciso primero del artículo 362 de la Constitución, la atención de salud como servicio público se prestará a través de las entidades estatales, privadas, autónomas, comunitarias y aquellas que ejerzan las medicinas ancestrales alternativas y complementarias. Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes;

El intercambio de información restringida dentro de la Universidad puede ser permitido si es necesario para satisfacer las necesidades legítimas de la universidad. Salvo que de lo contrario (O con fines de compartición entre las entidades encargadas de hacer cumplir la ley), no podrá divulgarse información restringida a las partes fuera de la Universidad, incluidos los contratistas, sin el consentimiento previo por escrito del receptor propuesto (i) tomar las medidas apropiadas para salvaguardar la confidencialidad del Información restringida; (ii) no revelar la Información Restringida a ninguna otra parte por ningún motivo

ausente el consentimiento previo por escrito de la Universidad o una orden judicial o citación judicial válida; Y (iii) notificar a la Universidad por adelantado de cualquier revelación de acuerdo con una orden judicial o citación, a menos que la orden o citatorio prohíba explícitamente dicha notificación. Además, el receptor propuesto debe cumplir con los requisitos de esta política. Cualquier intercambio de información restringida dentro de la Universidad debe cumplir con las políticas de la Universidad incluyendo Derechos, Reglas y Responsabilidades y Política de Uso Aceptable para Tecnología de la Información y Recursos Digitales de la Universidad de Yachay.

2. Confidencial

La información de la Universidad se clasifica como Confidencial si se encuentra fuera de la Clasificación restringida, pero no pretende ser compartida libremente dentro o fuera de la Universidad debido a su naturaleza sensible y/o obligaciones contractuales o legales. Ejemplos de información confidencial incluyen toda la información no restringida contenida en archivos de personal, registros de investigaciones de mala conducta y de aplicación de la ley, datos financieros internos, registros de donantes y registros de educación (según lo definido por LOES u otros).

3. Sin restricciones en Yachay Tech (SRY)

La información de la Universidad está clasificada Sin restricciones dentro de Yachay Tech (SRY) si no está dentro de las clasificaciones Restringida y Confidencial, pero no está destinada a ser compartida libremente fuera de la Universidad. Un ejemplo redes sociales (Facebook, Twitter, etc).

La suposición es que la información SRY permanecerá dentro de la Universidad Yachay Tech. Sin embargo, esta información se puede compartir fuera de Yachay Tech si es necesario para satisfacer las necesidades empresariales legítimas de la Universidad, y el destinatario propuesto acepta no volver a divulgar la información sin el consentimiento de la Universidad.

4. Pública

La información universitaria está clasificada como Pública si está destinada a estar disponible para cualquier persona dentro y fuera de la Universidad Yachay.

B. Protección, manejo y clasificación de la información

1. En función a la clasificación, la información universitaria debe estar adecuadamente protegida contra el acceso no autorizado, la pérdida y el daño. Los requisitos específicos de seguridad para cada clasificación se pueden encontrar en las Normas y Procedimientos de Protección de la Información de Yachay.
2. El manejo de Información Universitaria de cualquier fuente que no sea la universidad Yachay Tech puede requerir el cumplimiento tanto de esta política como de los requisitos de la persona o entidad que creó, proporcionó o controló la información. Si tiene dudas sobre su capacidad de cumplimiento, consulte al Asesor Legal.
3. Cuando se considere apropiado, se puede aumentar el nivel de clasificación o imponer requisitos de seguridad adicionales más allá de lo requerido por la Política de Seguridad de la Información y las Normas y Procedimientos de Protección de la Información de Yachay Tech.

V. Responsabilidades

Se espera que todos los profesores, el personal administrativo, los estudiantes de la universidad Yachay Tech (cuando actúen en nombre de la Universidad a través del servicio en los cuerpos de la Universidad) y otros que hayan recibido el uso de la información universitaria:

- Comprender los niveles de clasificación de información definidos en la Política de seguridad de la información.
- Según corresponda, clasifique la información de la cual uno es en consecuencia responsable.
- Acceder a la información solo si es necesario para satisfacer las necesidades comerciales legítimas.
- No divulgar, copiar, liberar, vender, prestar, alterar o destruir ninguna información de la Universidad sin un propósito comercial válido y/o autorizado.
- Proteger la confidencialidad, la integridad y la disponibilidad de la información de

la Universidad de manera coherente con el tipo y nivel de clasificación de la información.

- Manejar la información de acuerdo con los Estándares y Procedimientos de Protección de la Información de Yachay Tech y cualquier otra norma o política aplicable de la Universidad.
- Proteja cualquier llave física, tarjeta de identificación, PIN, cuenta de computadora o cuenta de red que le permita a uno acceder a la información de la Universidad.
- Descartar los medios que contienen información de la Universidad Yachay Tech de manera consistente con el nivel de clasificación de la información, el tipo y cualquier requisito de retención de la Universidad aplicable. Esto incluye información contenida en cualquier documento impreso (como una nota o informe) o en cualquier medio de almacenamiento electrónico, magnético u óptico (como una tarjeta de memoria, CD, disco duro, cinta magnética o disco).
- Póngase en contacto con la Oficina del Asesor Jurídico antes de divulgar la información generada por esa Oficina o antes de responder a cualquier citación o citaciones judiciales, órdenes judiciales u otras solicitudes de información de litigantes privados y entidades gubernamentales.
- Póngase en contacto con la oficina universitaria correspondiente antes de responder a las solicitudes de información de las agencias reguladoras, inspectores, examinadores y / o auditores.

VI. Políticas, procedimientos, estándares y plantillas de Yachay Tech relacionados

- Derechos, Reglas, Responsabilidades
- Política de uso aceptable para tecnología de la información y recursos digitales de Universidad de Yachay Tech.
- Política de la Universidad para aceptar y manejar la política de contratación pública.
- Política sobre compras internacionales
- Política sobre compras de Hardware y Software
- Los Procedimientos de Alertas bajo la Universidad de Yachay Tech son el Programa de Prevención de Robo de Identidad.
- Procedimiento para responder a una posible exposición de datos confidenciales de la Universidad.
- Plantilla de Acuerdo de Confidencialidad.

VII. Política de Revisión

Como mínimo, la Política de seguridad de la información se revisará cada 12 meses.

ANEXO VI

PROCEDIMIENTO DE AUDITORÍAS INTERNAS

1. Objetivo

El objetivo de la auditoria interna es identificar, verificar y medir la eficacia del sistema implementado por la empresa con miras a realizar un correcto mantenimiento continuado y evolutivo del SGSI.

Este documento establece los lineamientos y los procedimientos a seguir para la planificación y realización de la auditoria interna del SGSI de la empresa, y así también los reportes de resultados de la evaluación

2. Alcance

Este procedimiento es aplicable a todas las auditorias de los procesos de la empresa enmarcados dentro del SGSI.

A continuación, se describe el perfil del auditor interno, una planificación, así como un modelo de informe de auditorías internas:

3. Perfil del Auditor Interno

El auditor interno es la persona encargada de realizar periódicamente la auditoría interna en la institución. Es su responsabilidad la coordinación entre todas las partes implicadas, realizar un correcto registro de todos los elementos auditables y en resumen planificar, preparar y realizar las auditorías internas.

Las funciones específicas del auditor interno son:

- Planificar las auditorías.
- Comunicar e instituir los requisitos de la auditoría.
- Conocer y considerar los resultados de las auditorías anteriores, en caso de haber.
- Dirigir el proceso de auditoría en el período planificado.

- Recoger evidencias objetivas del área auditada, mediante entrevistas, observación de actividades y revisión de registros.
- Comprobar que el sistema de gestión de seguridad de la información está conforme con la norma, se encuentre vigente y eficaz.
- Informar de forma eficaz y eficiente a los implicados los hallazgos obtenidos durante la auditoría.
- Documentar de forma adecuada las observaciones y no conformidades.
- Elaborar y presentar el informe de auditoría.

El auditor interno debería poseer título universitario en el área de la Ingeniería Informática o de Telecomunicaciones, deberá haber realizado el curso de auditor interno ISO 27001 y experiencia en la ejecución de auditorías de Sistemas de Gestión de la Seguridad de la Información.

4. Programa de Auditoria

Se planificará la realización de auditorías parciales (por control previsto en la normativa ISO 27002), realizando la auditoría de acuerdo al programa de auditoria a lo largo de un año.

La planificación inicial de auditorías de seguridad es la siguiente:

AUDITORIA	PERIODO											
CONTROL	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10	MES 11	MES 12
5 POLITICAS DE SEGURIDAD			X									
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION			X									
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			X									
8 GESTION DE ACTIVOS						X						
9 CONTROL DE ACCESO						X						
10 CIFRADO						X						
11 SEGURIDAD FISICA Y AMBIENTAL									X			
12 SEGURIDAD EN LA OPERATIVA.									X			
13 SEGURIDAD EN LAS TELECOMUNICACIONES.									X			
14 ADQUISICION , DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION												X
15 RELACIONES CON SUMINISTRADORES.												X
16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION												X
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO												X
18 CUMPLIMIENTO												X

Cuadro 5: Programa de Auditoria.

5. Informe de Auditoria

Existen diversas inconformidades que se detectan en una auditoria, que se presentan de acuerdo a las experiencias, conocimientos y necesidades del responsable de hacer la auditoria.

Además, que cada proveedor que realiza un trabajo de auditoria, tienen establecidas sus propias formas de reportar las observaciones, estandarizando así la forma de elaborar su informe de auditoría.

Podemos tomar dos formatos de auditoria que son prácticos, por la forma que ayudan al auditor a reportar las inconformidades encontradas en la auditoria, con la finalidad de que la persona lectora entienda lo que se está informando en estos documentos, esto facilita a:

- La forma de reportar las inconformidades observadas en la evaluación.
- Para enseñar a los auditores principiantes como elaborar informes de auditoría, pues son fáciles de llenar y comprender.

A continuación, se presentan modelos de documentos tanto para el programa, el plan y el informe de las auditoria:

INFORME DE AUDITORIA INTERNA

Fecha: / /

PLAN DE AUDITORIA INTERNA FECHA: / /

PROGRAMA ANUAL DE AUDITORIA

I DATOS GENERALES

Norma de referencia | Año :

Objetivo

II PROGRAMA DE AUDITORIAS

N°	Proceso/Área	Mes/Semanas																																															
		Ene				Feb				Mar				Abr				May				Jun				Jul				Ago				Sep				Oct				Nov				Dic			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
N° de Auditorias																																																	
Total de auditorias																																																	

II PROGRAMA DE AUDITORIAS

Elaborado por:	Aprobado por:
Nombre, cargo y firma	Nombre, cargo y firma
Fecha: / /	Fecha: / /

ANEXO VII

GESTIÓN DE INDICADORES

A continuación, se definen una serie de indicadores para medir la gestión y el cumplimiento en el avance de la implementación del SGSI:

1. Organización de Seguridad de la Información
2. Cobertura del SGSI en activos de información
3. Tratamiento de eventos relacionados con el SGSI
4. Plan de Sensibilización
5. Políticas de Seguridad de la Información
6. Cumplimiento de políticas de Seguridad de la Información
7. Verificación de Control de Acceso
8. Implementación de los procesos de registro y auditoria
9. Implementación de Controles

ID	IND-SGSI-01
Nombre	Organización de Seguridad de la Información
Descripción	Indicador que permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a la seguridad de la información, en lo relacionado con asignación roles, perfiles y responsabilidades relacionados con la seguridad de la información al interior de la entidad.
Control de Seguridad	A .7 .1.2, A .13.2.4
Medida	(Número de personas con su respectivo acuerdo/Número total de personas que deben tener acuerdos con la institución)*100.
Unidad de Medida	porcentual
Frecuencia	anual
Valor Objetivo	100%
Valor limite	>=80%
Responsable	Talento Humano y Jurídico

Cuadro 6: Indicador 1 Organización de Seguridad de la Información

ID	**IND-SGSI-02**
Nombre	Cobertura del SGSI en activos de información
Descripción	Indicador que permite determinar y hacer seguimiento, a la cobertura que se realiza a nivel de activos críticos de información de la entidad y los controles aplicados.
Control de Seguridad	A .8.1 .1, A .8.1 .3
Medida	(Número de activos críticos de información con controles/Número total de activos críticos de información de la entidad)*100.
Unidad de Medida	porcentual
Frecuencia	semestral
Valor Objetivo	100%
Valor limite	>=80%
Responsable	Responsable del SI y TIC

Cuadro 7: Indicador 2 Cobertura del SGSI en activos de información

ID	**IND-SGSI-03**
Nombre	Tratamiento de eventos relacionados con el SGSI
Descripción	Indicador que permite determinar la eficiencia en el tratamiento de eventos relacionados al SGSI. Los eventos serán reportados por los usuarios o determinados en las auditorias planeadas para el sistema.
Control de Seguridad	A .12.4.1, A .12.4.3
Medida	(Número de eventos cerrados/Número total de eventos reportado y encontrados)*100.
Unidad de Medida	porcentual
Frecuencia	semestral
Valor Objetivo	100%
Valor limite	>=80%
Responsable	Responsable del SI y TIC

Cuadro 8: Indicador 3 Tratamiento de eventos relacionados con el SGSI

ID	**IND-SGSI-04**
Nombre	Plan de Sensibilización
Descripción	Indicador que permite determinar la eficiencia en el tratamiento de eventos relacionados al SGSI. Los eventos serán reportados por los usuarios o determinados en las auditorias planeados para el sistema.
Control de Seguridad	A .7.2.2
Medida	(Número de personas sensibilizadas/Número total de personas a capacitar)*100.
Unidad de Medida	porcentual
Frecuencia	semestral
Valor Objetivo	100%
Valor limite	>=80%
Responsable	Responsable del SI y TIC

Cuadro 9: Indicador 4 Plan de Sensibilización

ID	**IND-SGSI-05**
Nombre	Políticas de Seguridad de la Información
Descripción	Indicador que permite determinar el grado de implementación de las políticas de confidencialidad, disponibilidad e integridad de la información.
Control de Seguridad	5.2, 6.2
Medida	La entidad ha implementado lineamientos, normas y/o estándares con la finalidad de proteger la información personal y privada de los estudiantes.
Unidad de Medida	booleano
Frecuencia	semestral
Valor Objetivo	VERDADERO
Valor limite	NA
Responsable	Responsable del SI y TIC

Cuadro 10: Indicador 4 Políticas de Seguridad de la Información	
ID	**IND-SGSI-06**
Nombre	Cumplimiento de políticas de Seguridad de la Información
Descripción	Indicador que permite determinar el cumplimiento de políticas de seguridad de la información en la entidad.
Control de Seguridad	A6.1, A .1 8.1.1
Medida	* La entidad ha definido una política general de seguridad de la información. * La entidad ha definido una organización en términos de roles y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades. *La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información.
Unidad de Medida	booleano
Frecuencia	semestral
Valor Objetivo	VERDADERO
Valor limite	NA
Responsable	Responsable del SI y TIC

Cuadro 11: Indicador 6 Cumplimiento de políticas de Seguridad de la Información	
ID	**IND-SGSI-07**
Nombre	Verificación de Control de Acceso
Descripción	Indicador que permite identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso.
Control de Seguridad	A .9.1.1
Medida	* La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad. * La entidad ha definido lineamientos, normas y/o estándares

	para controlar las terminales móviles y accesos remotos a los recursos de la entidad.
Unidad de Medida	booleano
Frecuencia	semestral
Valor Objetivo	VERDADERO
Valor limite	NA
Responsable	Responsable del SI y TIC

Cuadro 12: Indicador 7 Verificación de Control de Acceso

ID	**IND-SGSI-08**
Nombre	Implementación de los procesos de registro y auditoria
Descripción	Indicador que permite verificar la existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.
Control de Seguridad	9.1, 9.2
Medida	* La entidad ha definido lineamientos, normas y/o estándares para el registro y control de eventos que suceden sobre sus sistemas, redes y servicios. * La entidad verifica de manera interna y/o a través de terceros, periódicamente sus procesos de seguridad de la información y sistemas para asegurar el cumplimiento del SGSI.
Unidad de Medida	booleano
Frecuencia	semestral
Valor Objetivo	VERDADERO
Valor limite	NA
Responsable	Responsable del SI y TIC

Cuadro 13: Indicador 8 Implementación de los procesos de registro y auditoria

ID	**IND-SGSI-09**
Nombre	Implementación de Controles
Descripción	Indicador que permite determinar el grado de avance en la implementación de controles de seguridad.
Control de Seguridad	6.1 .3 e), 6.2
Medida	(Número de controles implementados/Número total de controles que se planearon implementar)*100.
Unidad de Medida	porcentual
Frecuencia	semestral
Valor Objetivo	100%
Valor limite	>=80%
Responsable	Responsable del SI y TIC

Cuadro 14: Indicador 9 Implementación de Controles

ANEXO VIII

PROCEDIMIENTO REVISIÓN POR DIRECCIÓN

1. Introducción

La dirección de la institución toma a cargo la revisión del SGSI. Es a través de esta revisión que la dirección busca garantizar que el Sistema de Gestión de Seguridad de la Información funcione de manera segura, continua y de mejoramiento continuo.

La revisión incluye la evaluación de las oportunidades de mejora y la necesidad de realizar cambios en el SGSI. En esta revisión se incluye la política de seguridad de la información y los objetivos de seguridad de la información.

2. Objetivo

El objetivo de estos documentos es especificar el conjunto de acciones que la Dirección de la empresa debe realizar en el proceso de revisión de los procedimientos y los controles implementados.

3. Alcance

La Dirección es parte fundamental en la revisión del cumplimiento de los aspectos de seguridad relativa a la Información, por lo que se establece que:

- Realizar una revisión en intervalos planificados para asegurar la adecuación continua del SGSI, la mismas que debe ser por lo menos una vez al año.

- Se debe considerar el alcancé que tiene el SGSI en este caso es para todos los procesos relacionado con la parte Académica.

4. Proceso de la revisión

La revisión del SGSI estará por parte de la Dirección de la institución o un Comité responsable de la administración del sistema de gestión, verificando los siguientes puntos:

- Las Políticas de calidad y seguridad de la información.
- El cumplimiento de los objetivos de calidad y seguridad de la información.
- El desempeño de los procesos y conformidad de los productos, incluyendo la retroalimentación de las partes interesadas.
- Los resultados de las auditorías internas y externas.
- Las acciones correctivas y preventivas necesarias para el mejoramiento del SGSI.
- Cumplimiento de la implementación de los planes de tratamiento definidos para los riesgos identificados.
- Resultados de las mediciones de eficacia del SGSI.
- Cambios y requerimientos organizacionales que podrían afectar al Sistema de Gestión.
- Resultados de la gestión de riesgos corporativos, incluyendo vulnerabilidades o amenazas.

La revisión en este caso lo realizar un comité de revisión que estará compuesto por el Responsable de la Seguridad de la Información, el Director de Talento Humano y la Dirección de la institución.

Se fija una reunión anual con la Alta Dirección para proporcionarle una visión general de alto nivel del estado de funcionando el sistema.

Para realizar esta revisión es necesario contar con la siguiente información:

1. Estado de acciones basadas en revisiones anteriores, en caso de existir.
2. Un reporte de los cambios en los asuntos externos e internos pertinentes al SGSI
3. Retroalimentaciones sobre:
    a. Las conformidades y acciones correctivas
    b. Resultados de monitoreo y mediciones
    c. Resultados de auditorias
    d. El cumplimiento de los objetivos de la seguridad de la información
4. Los resultados obtenidos de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.
5. Cambios en el contexto de la empresa que afecten al SGSI, como el cambio de estrategia de la organización.
6. Comentarios de las partes implicadas que consten entre cada revisión de la Dirección.
7. Oportunidades de mejora referentes al SGSI.
8. Se ha de conservar la información documentada de forma detallada como evidencia de revisión.

9. Como salidas de la revisión de Dirección se consideran las decisiones relacionadas con oportunidades de mejora y necesidades de cambio estratégicas.

Los resultados de esta revisión deben incluir decisiones o acciones que estén relacionadas:

1. Con las oportunidades de mejora continua
2. Mejoras en la eficacia del SGSI
3. Actualización del plan de evaluación de riesgos y del tratamiento de riesgos
4. Necesidades de cambios al SGSI (procesos y controles)
5. Necesidades de recursos

Los resultados obtenidos de las revisiones serán documentados y registrados en las actas de las reuniones.

Acciones de la agenda de la reunión de la revisión

1. Introducción
   a. Propósito de la reunión
   b. Revisión de la lista de asistentes, se debe tener la certeza de que las personas clave estén presentes.
2. Acciones de revisión de las Actas
   a. Revisión de actas de reuniones anteriores
   b. Verificar el estado de las acciones con los asistentes
   c. Registro del estado actual del SGSI frente a las acciones en curso d. Cierre de las acciones completadas
3. SGSI y Gestión de Riesgos
   a. Revisar / confirmar el alcance y los objetivos del SGSI
   b. Revisar el desempeño del SGSI y la mejora continua
   c. Revisar restricciones de recursos, presupuestos y otras cuestiones d. Revisar el registro de riesgos y los riesgos abiertos / cerrados
   d. Discutir políticas y procedimientos de seguridad de la información
4. Métricas de rendimiento / KPI
   a. Revisar métricas de rendimiento y KPI
   b. Discutir los resultados de incidentes recientes y respuesta
5. Reunión Cierre
   a. Confirmar las acciones y los propietarios de las acciones
   b. Confirmar plazos para acciones
   c. Confirmar fecha y hora de la próxima reunión, propósito, los participantes, los temas a tratar.
   d. Otros

A continuación, se dispones de los documentos a ser utilizados para la reunión de revisión de la dirección y las actas de las reuniones.

AGENDA DE LA REUNIÓN DE REVISIÓN Y ACTA DE LA REUNIÓN

PARTICIPANTES

REUNION DE REVISION DE LA DIRECCION REV

Fecha	**Hora**	**Lugar**

Presidente reunión	**Moderador**	**Secretario actas**	**Expositor**

PREPARACIÓN:

ENTRADAS:

OBJETIVO:

TEMAS AGENDA

PROXIMA REUNION

Fecha	**Hora**	**Lugar**	
Presidente reunión	**Moderador**	**Secretario actas**	**Expositor**

ACTA DE LA REUNION DE REVISION **FECHA: / /**

ITEM AGENDA	RESULTADOS/DECISIONES	ACCION A EJECUTAR, COMUNICACIONES	RESPONSABLE	FECHA DE VENCIMIENTO	ESTADO
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

RESUMEN DE RESULTADOS DE LA REUINION

Fecha de la siguiente reunión: / /

Firma: …… Fecha: / / **Firma: …… Fecha: / /**

Director de la reunión **Representante de la Dirección**

ANEXO IX

GESTIÓN DE ROLES Y RESPONSABILIDADES

La Política de Seguridad de la información debe definir responsables generales de cada una de las áreas.

La Política de Seguridad de la información debe apoyarse en políticas específicas para las cuales se debe definir responsables específicos, entre estas políticas específicas podemos enumerar las siguientes:

- Control de accesos
- Clasificación de la información
- Seguridad física y ambiental
- Concernientes al usuario final
- Copias de seguridad
- Transferencia de la información
- Protección ante software malicioso y otros ataques informáticos
- Gestión de vulnerabilidades técnicas
- Criptografía
- Seguridad de las comunicaciones
- Protección de datos de carácter personal
- Relaciones con proveedores

Adicionalmente deberán estar definidos responsables, en el ámbito de la Seguridad de la información, sobre activos, operacionales que valen por el detalle de los procedimientos operativos para llevar a cabo diferentes tareas, para la gestión ante incidentes de Seguridad de la información cuando estos ocurran, a nivel legislativo y regulatorio.

La Dirección de la empresa ha de tener en cuenta la siguiente organización base:

Comité de Seguridad de la información será integrado, por una parte, del equipo directivo de la institución y por otra por los responsables de cada una de las áreas impactadas por los activos y procesos definidos:

- CISO – Chief Information Security Officer como Gestión de la Seguridad de la Información
- CIO – Chief Information Officer como gerente de sistemas o director de tecnologías de la información, siendo un cargo operacional. Este reporta directamente al CEO.
- CTO – Chief Technology Officer en un rol similar al CIO pero más técnico y que reporta a éste.
- Responsable del Departamento Jurídico.
- Responsable de la parte académica (Cancillería).

- Responsable de Talento Humano
- Representantes de las diferentes áreas y/o personas con responsabilidades en el ámbito de la Seguridad de la Información (mencionados anteriormente).

Pero no todos los roles estarán dentro del comité de seguridad de la información. Las responsabilidades del Comité son:

- Responsable de revisar y aprobar la política de seguridad de la información.
- Encargado de la definición de las políticas, normas y procedimientos relacionados con la seguridad de la información e igualmente velarán por la implantación y cumplimiento de los mismos.
- Comunicar y promover estas políticas dentro de la organización: objetivos, principios, responsabilidades.
- Identificar activos y procesos de Seguridad de la información y designar responsables para cada uno.
- Definir los diferentes niveles y procesos de autorización.
- Analizar, estructurar e implementar los diferentes programas de Seguridad de la información.
- Coordinar decisiones de seguridad, normas, análisis de riesgos, planes de continuidad, planes de recuperación de desastres, etc.
- Asegurar el lineamiento de las Políticas de Seguridad de la información de la organización con la legislación vigente.

ANEXO X

METODOLOGÍA DE ANÁLISIS DE RIESGOS

En la presente metodología se ha estipulado 7 pasos para determinar la matriz de riesgo de la Seguridad de la Información:

Primero. - Caracterización del Sistema

En esta parte se tiene que identificar y valorar los activos valiosos para la empresa.

La valoración puede ser de forma cuantitativa o cualitativa en este caso vamos a valorar de forma cualitativa teniendo en cuenta el costo de cada activo, adicionando los valores de criticidad y tiempos de reposición y de ejecución, ver tabla 15.

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

Cuadro 15: Tabla de valoración de activos.

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

Cuadro 16: Tabla de valoración para las dimensiones de seguridad.

Segundo. - Identificación de las amenazas

Se procede a identificar las amenazas a las que esta expuestos los activos.

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).

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
[E.7]	Errores y fallos no intencionados	Deficiencias en la organización

[E.8]	Errores y fallos no intencionados	Difusión de software dañino
[E.9]	Errores y fallos no intencionados	Errores de [re-]encaminamiento
[E.10]	Errores y fallos no intencionados	Errores de secuencia
[E.14]	Errores y fallos no intencionados	Escapes de información
[E.15]	Errores y fallos no intencionados	Alteración accidental de la información
[E.18]	Errores y fallos no intencionados	Destrucción de información
[E.19]	Errores y fallos no intencionados	Fugas de información
[E.20]	Errores y fallos no intencionados	Vulnerabilidades de los programas (software)
[E.21]	Errores y fallos no intencionados	Errores de mantenimiento / actualización de programas (software)
[E.23]	Errores y fallos no intencionados	Errores de mantenimiento / actualización de equipos (hardware)
[E.24]	Errores y fallos no intencionados	Caída del sistema por agotamiento de recursos
[E.25]	Errores y fallos no intencionados	Pérdida de equipos
[E.28]	Errores y fallos no intencionados	Indisponibilidad del personal
[A.3]	Ataques intencionados	Manipulación de los registros de actividad (log)
[A.4]	Ataques intencionados	Manipulación de la configuración
[A.5]	Ataques intencionados	Suplantación de la identidad del usuario
[A.6]	Ataques intencionados	Abuso de privilegios de acceso

[A.7]	Ataques intencionados	Uso no previsto
[A.8]	Ataques intencionados	Difusión de software dañino
[A.9]	Ataques intencionados	[Re-]encaminamiento de mensajes
[A.10]	Ataques intencionados	Alteración de secuencia
[A.11]	Ataques intencionados	Acceso no autorizado
[A.12]	Ataques intencionados	Análisis de tráfico
[A.13]	Ataques intencionados	Repudio
[A.14]	Ataques intencionados	Interceptación de información (escucha)
[A.15]	Ataques intencionados	Modificación deliberada de la información
[A.18]	Ataques intencionados	Destrucción de información
[A.19]	Ataques intencionados	Divulgación de información
[A.22]	Ataques intencionados	Manipulación de programas
[A.23]	Ataques intencionados	Manipulación de los equipos
[A.24]	Ataques intencionados	Denegación de servicio
[A.25]	Ataques intencionados	Robo
[A.26]	Ataques intencionados	Ataque destructivo
[A.27]	Ataques intencionados	Ocupación enemiga
[A.28]	Ataques intencionados	Indisponibilidad del personal
[A.29]	Ataques intencionados	Extorsión
[A.30]	Ataques intencionados	Ingeniería social (picaresca)

Cuadro 17: Clasificación 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

Cuadro 18: Tabla de Frecuencia

Tercero. - Análisis de Impacto

En este paso vamos a relacionar las amenazas que pueden tener éxito, antes debemos tener en cuenta nuestros activos clasificados.

Para determinar el impacto es necesario determinar el grado de degradación que puede tener el activo en términos de seguridad: Disponibilidad, Integridad y Confidencialidad.

Se debe establecer la magnitud del impacto se debe tener en cuenta que el impacto puede ser tangible utilizando métodos cuantitativos estableciendo costos, o también puede ser cualitativo de una manera subjetiva. Para esto se determinó 3 categorías alto, medio y bajo, a continuación, se describe:

Definición de Impacto	
Alta	Acción de la vulnerabilidad debe resultar una perdida con altos costos en los activos o recursos tangibles críticos; debe significar violación, perjuicio, o impedir la misión, reputación o interés de la organización; o debe resultar en muerte humana o serias injurias
Media	Acción de la vulnerabilidad debe resultar una pérdida de costos en los activos o recursos tangibles; debe significar violación, perjuicio, o impedir la misión, reputación o interés de la organización; o debe resultar en injurias.

Baja	Acción de la vulnerabilidad debe resultar en la pérdida de algún activo o recurso tangible; o afecta notablemente en la misión, reputación o interés de la organización.

Cuadro 19: Magnitud del Impacto

Para este ejercicio se ha decidido aplicar el método cualitativo para lo cual se tiene el siguiente cuadro que relaciona el impacto con la degradación.

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

Cuadro 20: Matriz de nivel de Impacto

Cuarto. - Determinar el Riesgo

Para este paso se valora el nivel de riesgo para el sistema de TI. Se determinará el riesgo que probabilidad que tenga una amenaza/vulnerabilidad.

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

frecuencia en una tabla para calcular el riesgo: ***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

Cuadro 21: Matriz de nivel de riesgo

Quinto- Análisis de Control (Salvaguardas)

El objetivo de este paso es identificar los controles que se tiene implementados o planeados implementar, para minimizar o eliminar la probabilidad que una amenaza se concrete.

Sexto- Impacto Residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su 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.

Séptimo. - Riesgo Residual

Dado un cierto conjunto de salvaguardas 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.

Para el paso 6 y 7 se vuelven a realizar los cálculos realizados en paso 3 y 4 respectivamente.

ANEXO XI.

DECLARACIÓN DE APLICABILIDAD

A continuación, se muestra la matriz de aplicabilidad por dominio y control:

L: Requerimiento Regulatorio

C: Obligación contractual

N: Requerimiento del negocio

R: Análisis de riesgos

			Salvaguardas Seleccionadas		**Razones para la selección de los controles**			
Sección	**Controles ISO 27002:2013**	**Justificación para exclusión**	**Salvaguardas existentes**	**Salvaguardas planeadas**	**L**	**C**	**N**	**R**
5	Política de seguridad							
5.1	Política de seguridad de la información							

5.1.1	Conjunto de políticas para la seguridad de la información		Existen políticas de uso de Internet documentada y vigente.	Redactar el documento: “Política de Seguridad de la Información” (PSI)	**x**		**x**	
5.1.2	Revisión de la Política de Seguridad de la Información		Actualmente no se cuenta con un procedimiento claro al respecto.	Redactar un documento: “Política de Seguridad de la Información” se establece un procedimiento de revisión de la política de seguridad	**x**		**x**	
6	Aspectos Organización de la seguridad de la información							
6.1	Organización Interna							
6.1.1	Asignación de Responsabilidades para la Seguridad de la Información		Las responsabilidades no son conocidas en la organización	En el documento: “Política de Seguridad de la Información”, se establecerá las responsabilidades frente a la seguridad de la información.			**x**	

6.1.2	Segregación de tareas.		No se tiene segregada las tareas.	En el documento: “Política de Seguridad de la Información” se plasmara el compromiso manifiesto de las máximas Autoridades de la institución y de los Jefes de Área para la difusión, consolidación y cumplimiento de los principios de Seguridad que rigen a la institución. Se establecerá la conformación de un comité de seguridad de la información, conformado por miembros de distintos sectores de la organización.			**x**	
6.1.3	Contacto con la Autoridades		Existe un proceso de gestión legal y cumplimiento normativo en donde se establecen los procedimientos para gestionar las relaciones con las autoridades reguladoras	En el documento: “Política de Seguridad de la Información” se estipulara que el área de Control Interno de la institución. o la Auditoria de TI emitirá un informe Anual del estado y cumplimiento de las		**x**		

				normas de seguridad de la información.				
6.1.4	Contacto con Grupos de Interés Especial		Se mantiene contactos informales con proveedores de servicios de información	El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en la organización a fin de brindar ayuda en la toma de decisiones en materia de seguridad. (Documento Política de Seguridad de la Información)	**x**		**x**	
6.1.5	Seguridad de la información en la gestión de proyectos.		No se cuenta con un procedimiento al respecto.	Establecer documentación de procedimientos en donde se establece la metodología de actualización y creación de nuevos proyectos. Así mismo se establecerá el instructivo: Guía para la elaboración, manejo y control de proyectos.	**x**		**x**	
6.2	Dispositivos para movilidad y teletrabajo.							

6.2.1	Política de uso de dispositivos para movilidad.	La institución no cuenta con aplicaciones de informática móvil o de teletrabajo, para USB y portátiles se usa la política de medios extraíbles	NO APLICA	La institución no cuenta con aplicaciones de informática móvil o de teletrabajo, para USB y portátiles se usa la política de medios extraíbles				
6.2.2	Teletrabajo.	La institución no cuenta con aplicaciones de informática móvil o de teletrabajo	NO APLICA	La institución no cuenta con aplicaciones de informática móvil o de teletrabajo				
7	Seguridad ligada a los recursos humanos							
7.1	Antes de la contratación							

7.1.1	Investigación de Antecedentes		Se investigan los antecedentes para los candidatos a cargos en la organización	Se creara los procedimientos: PR-01 Contratación PR-02 Selección de personal Se establecerá el procedimiento de verificación de antecedentes para los candidatos y verificación de antecedentes a terceros.		**x**	**x**	
7.1.2	Términos y condiciones de Contratación			El departamento jurídico de la institución diseñara un contrato de confidencialidad que debe ser firmado por los funcionarios y los proveedores.			**x**	
7.2	Durante la contratación							
7.2.1	Responsabilidad de la gestión		La dirección reconoce a la seguridad con un factor decisivo en el negocio	Al inicio del contrato laboral, de debe dar a conocer el código de Seguridad de la Información de la institución y el documento: “Política de Seguridad de la Información”, el empleado, este se debe comprometer a cumplirlo junto			**x**	

				con las políticas de seguridad de la institución.				
7.2.2	Concienciación. Formación y capacitación en seguridad de la información			En el documento: “Política de Seguridad de la Información” se asignarán las responsabilidades de Capacitación. Adicionalmente los procedimientos e instructivos de usuario se constituyen en una herramienta adicional de capacitación.			**x**	
7.2.3	Procesos Disciplinario			Establecer sanciones por Incumplimiento del documento: “Política de Seguridad de la Información” se especificaran las sanciones previstas por incumplimiento de la Política de Seguridad de la Información.			**x**	
7.3	Cese o Cambio de Puesto de Trabajo							

7.3.1	Cese o Cambio de Puesto de Trabajo		se informa al área de sistemas el retiro de los funcionarios	Los jefes de área son los responsables de ejecutar la finalización de un empleo frente a funcionarios que estén a su cargo, el área de recursos humanos y administrativos está encargada de los trámites administrativos de la finalización del contrato. Establecer procedimientos para baja de usuarios.	**x**			
8	Gestión de activos							
8.1	Responsabilidad Sobre Los Activos							
8.1.1	Inventario de Activos		Se cuenta con un inventario de equipos y aplicaciones	En La institución existe un inventario actualizado con los activos de información de la compañía y su respectivo responsable. Adicionalmente el inventario de los activos de cómputo de la compañía se mantiene en el sistema y se especifica el	**x**		**x**	

				registro de nuevos activos como uno de los pasos del proceso Compras. En el procedimiento "Creación e ingreso de garantías al sistema" se describirá el proceso de administración del archivo de garantías de la compañía.				
8.1.2	Propiedad de los Activos		Se tiene identificado informalmente al responsable de los activos	En el "Inventario de Activos de Información" se establecerá los responsables de dichos activos de información.			**x**	
8.1.3	Uso aceptable de los Activos		Las regulaciones para el uso adecuado de la información y los activos para su administración, se encuentran documentadas en el manual de políticas de sistemas	En el documento: “Política de Seguridad de la Información” se establecerá las regulaciones para el adecuado manejo de la información según su clasificación			**x**	

8.1.4	Devolución de activos		Se solicita la devolución de tarjetas de acceso al finalizar el contrato	Al finalizar un contrato con la compañía, el área de recursos humanos y administrativos es responsable de verificar que todos los activos de la organización que estén en posesión empleados, contratistas y terceros sean devueltos.		**x**	**x**	
8.2	Clasificación de la Información							
8.2.1	Directrices de Clasificación			Se estableciera un sistema de clasificación de la información descrito en el "Documento Política de Seguridad de la información"	**x**		**x**	
8.2.2	Etiquetado y manipulación de la Información			Se creara el procedimiento de etiquetado y políticas que se encuentre documentado en el documento: “Política de Seguridad de la Información”			**x**	

8.2.3	Manipulación de activos		El servidor local de Carpeta Compartidas cuenta con las carpetas con listas de distribución a personas autorizadas. No se tiene normado la funcionalidad del Drive que se encuentra en la Nube.	Crear el proceso: Para la habilitación de usuarios en los sistemas de información, se definirá el procedimiento de autorización de acceso a las funciones de los distintos sistemas. - Crear un rol encargado del área de archivo que cuente con una lista de personas autorizadas para el préstamo de carpetas y el proceso de Solicitud de carpetas en el archivo" y creación de carpetas en el archivo"	x	x	**x**	x
8.3	Manejo de los soportes de almacenamiento.							
8.2.1	Gestión de soportes extraíbles.		La institución cuenta con un software que permite bloquear el uso de los puertos en las estaciones de trabajo. Lo que	Las políticas de gestión de medios extraíbles estarán estipuladas en el documento: "Política de Seguridad de la Información". Cuando por			**x**	**x**

			permitiría administrar las políticas.	motivos de trabajo los empleados requieran retirar información de la compañía se debe cumplir con lo estipulado en el procedimiento creado para el efecto.				
8.2.2	Eliminación de soportes.		Existe un procedimiento informal de retirada de soportes	En el documento: “Política de Seguridad de la Información” se creara un ítem donde se establecerá la eliminación de medios de información.			**x**	**x**
8.2.3	Soportes físicos en tránsito.		La documentación del sistema es de acceso limitado solo para el personal autorizado				**x**	
9	CONTROL DE ACCESO							
9.1	Requisitos de negocio para control de accesos							
9.1.1	Política de Control de Acceso		No se encuentran claramente definido las tareas y roles.	En el documento: “Política de Seguridad de la Información” se establecerá las políticas de	**x**		**x**	

				control de acceso de la compañía.				
9.1.2	Control de acceso a las redes y servicios asociados		La plataforma de red de la compañía cuenta con un software de seguridad que bloquea los accesos no autorizados en la red. La configuración y el acceso son controlados por el departamento de sistemas. Se comparte parte de red con la YACHAY E.P.	Crear procedimientos de alta y baja de usuarios en la red: Habilitación de usuarios en los sistemas de información Des habilitación de usuarios Crear procedimiento y políticas Control de Conexión a la Red			**x**	**x**
9.2	Gestión de acceso de usuario							
9.2.1	Gestión de altas/bajas en el registro de usuarios.		Se realiza una identificación individualizada de todos los usuarios	Crear procedimientos de alta y baja de usuarios: Habilitación de usuarios en los sistemas de información Des habilitación de usuarios	**x**		**x**	**x**

9.2.2	Gestión de los derechos de acceso asignados a usuarios		El sistema mantiene las autorizaciones de los usuarios Se cuenta con la opción de suspender temporalmente los privilegios	En el documento: “Política de Seguridad de la Información”, se establecerá el control de la asignación de privilegios.			**x**	**x**
9.2.3	Gestión de los derechos de acceso con privilegios especiales.		las contraseñas iniciales son únicas	Establecer en el documento: “Política de Seguridad de la Información” la Administración de Contraseñas de Usuario y la Administración de Contraseñas Críticas, se establece el proceso formal de gestión de contraseñas. Así mismo la Administración de contraseñas de la plataforma de información, están registrados los procedimientos de gestión de contraseñas de la institución.	**x**		**x**	**x**

9.2.4	Gestión de información confidencial de autenticación de usuarios.			En La institución se usa como procedimiento seguro de conexión los descritos en PSI "Camino Forzado". En PSI establecerá Registro de Usuarios, se establece que los usuarios tendrán un único identificador de acceso			**x**	
9.2.5	Revisión de los derechos de acceso de los usuarios.			Establecer en el documento: "Política de Seguridad de la Información" la Revisión de Derechos de Acceso de Usuarios: Los derechos de acceso son revisados por el área de Control Interno de la institución.	**x**			
9.3	Responsabilidades del usuario							
9.3.1	Uso de información confidencial para la autenticación		Cuando se entregan las contraseñas se da la información sobre el manejo de estas	En el documento: "Política de Seguridad de la Información" establecer el Uso de Contraseñas, se establecen las buenas prácticas que los			**x**	**x**

				usuarios de la institución deben tener con sus contraseñas.				
9.4	Control de acceso a sistemas y aplicaciones.							
9.4.1	Restricción del acceso a la información.		se segregan los grupos de usuarios en la red	La segregación de usuarios en las redes se encontrara en la PSI Control de Conexión a la Red				**x**
9.4.2	Procedimientos seguros de inicio de sesión.			La segregación de usuarios en las redes se encontrara en la PSI Control de Conexión a la Red				**x**
9.4.3	Gestión de contraseñas		La institución cuenta con un sistema de gestión de contraseñas interactivo que promueve el cumplimiento de las políticas de contraseñas establecidas	En el documento: “Política de Seguridad de la Información” establecer el Uso de Contraseñas, se establecen las buenas prácticas que los usuarios de la institución deben tener con sus contraseñas.				**x**

9.4.4	Uso de herramientas de administración de sistemas			En PSI se establecerá que: Los usuarios finales y los operadores por ningún motivo tendrán acceso a programas fuente, ni a utilitarios de uso de desarrollo, ni a líneas de comando			**x**	**x**
9.4.5	Control de acceso al código fuente de los programas		La restricción de accesos se da a los sistemas desarrollados internamente, mediante la custodia del Jefe de Área.	La política de accesos se encontrara documentada en PSI Registro de Usuarios			**x**	**x**
10	Cifrado							
10.1	Controles criptográficos							
10.1.1	Política de uso de los controles criptográficos			En el PSI se establecerá la Política de Utilización de Controles Criptográficos.	**x**		**x**	
10.1.2	Gestión de claves			En el PSI se establecerá la Administración de claves criptográficas	**x**		**x**	
11	Seguridad física y del entorno							

11.1	Áreas seguras							
11.1.1	Perímetro de Seguridad Física		Las instalaciones de La institución con los siguientes controles de acceso físico: tarjetas de acceso, paredes sólidas y un puesto de recepción	Establecer un documento con las áreas protegidas.			**x**	
11.1.2	Controles Físicos de Entrada			Los controles de las áreas de seguridad se detallaran en el documento: “Política de Seguridad de la Información”			**x**	
11.1.3	Seguridad de Oficinas, despachos e instalaciones		Existe una institución de seguridad encargada de la protección de las instalaciones.	Los controles de las áreas de seguridad se detallaran en el documento: “Política de Seguridad de la Información”			**x**	

11.1.4	Protección contra las amenazas externas y de origen ambiental		La institución cuenta con un programa de brigadas de acción en caso de emergencia Implementos de seguridad ambiental y física a. Extintor de ABC b. Sistema de aire acondicionado c. Red regulada de voltaje d. Detector de humo y/o incendio e. Cableado estructurado f. Puerta de acceso con seguridad.	Establecer un inspección especializada para constatar el funcionamiento. Establecer el área responsable del mantenimiento de las áreas físicas.			**x**	
11.1.5	Trabajo en Áreas seguras		La institución cuenta con un ambiente informático propio.	En PSI se establecerá la disposición de un entorno dedicado para las aplicaciones sensibles: Aislamiento de los			**x**	**x**

				Sistemas Sensibles				
11.1.6	Áreas de acceso público, carga y descarga		Las áreas de carga y descarga se encuentran fuera de las instalaciones de la institución.	En el documento: “Política de Seguridad de la Información” se dictarán las normas para recepción y distribución.			**x**	
11.2	Seguridad de los equipos							
11.2.1	Emplazamiento y protección de los equipos			Se creara el procedimiento de Instalación de equipos de cómputo se define el procedimiento seguro para realizar la instalación de equipos.			**x**	**x**
11.2.2	Instalaciones de suministros		El edificio cuenta con dos plantas de energía accionadas automáticamente en caso de interrupción eléctrica, que se encuentran en El Rosario y San José.	La institución repotenciara los UPS que funciona en caso de presentarse una falta de energía.			**x**	

11.2.3	Seguridad del Cableado			Se contratara una empresa para la certificación del cableado estructurado.			**x**	**x**
11.2.4	Mantenimiento de los Equipos		El mantenimiento a los equipos se hace de acuerdo a la garantía por personal debidamente autorizado	El mantenimiento de la plataforma tecnológica se encontrara documentado en los procesos: Solicitud de Soporte Técnico Mantenimiento de los equipos de cómputo En el "Documento Política de Seguridad de la Información" se establecerá la normatividad de mantenimiento de equipos de la institución.			**x**	**x**
11.2.5	Salida de activos fuera de las dependencias de la empresa.			Las medidas a seguir para equipamiento fuera de la instalaciones de la compañía se encentrarán descritas en el documento: “Política de Seguridad de la				

				Información". Se creara el procedimiento Transporte equipos de cómputo, se establecerá el correcto envío y entrega de equipos de cómputo a las sucursales de la institución.				
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones			Se creará el procedimiento "Trasporte de equipos" se establece el sistema de autorización de retiro de equipos de la compañía. Se creará el procedimiento "Autorización de retiro de información de la compañía" se especifica la autorización de retiro de información de la compañía.	**x**	**x**	**x**	**x**

11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.			En el documento: “Política de Seguridad de la Información” se establecerá que: Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar.			**x**	**x**
11.2.8	Equipo informático de usuario desatendido			La protección de los equipos desatendidos se encontrará publicada en el documento: “Política de Seguridad de la Información” - Equipos Desatendidos en Áreas de Usuarios.				**x**
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla			Registro de políticas en el documento Política de Seguridad de la información. numeral 5.15 “Políticas de				**x**

				Escritorios y Pantallas Limpias".				
12	Seguridad en la Operatividad							
12.1	Procedimientos y responsabilidades de operación							
12.1.1	Documentación de los Procedimientos de Operación			Se creará los documentos: Documentación de procedimientos Guía para la elaboración, manejo y control de documentos			**x**	**x**
12.1.2	Gestión de Cambios			El control de cambios de los sistemas de información se estipulará en los siguientes procedimientos: Elaboración del requerimiento Desarrollo del requerimiento En el documento: "Política de Seguridad de la Información" se encuentran las políticas de	**x**		**x**	**x**

				gestión de cambios de la organización.				
12.1.3	Gestión de capacidades.		Los roles están segregados informalmente	las funciones de los cargos del área de sistemas se encuentran documentados en el manual de funciones. En el documento de política de seguridad de la información se definirá los controles de separación de funciones.	**x**		**x**	
12.1.4	Separación de entornos de desarrollo, prueba y producción.		Se impide el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.	En el documento de política de seguridad de la información se realiza una definición formal de los entornos de desarrollo: La compañía cuenta con tres ambientes separados para efectuar el desarrollo de sus sistemas de información:	**x**		**x**	**x**

				desarrollo, pruebas y producción. Se utilizarán sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Se prohíbe a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión. El paso de información entre los diferentes ambientes de desarrollo se documentarán en el procedimiento: Desarrollo del requerimiento				
12.2	Protección contra software malicioso y código móvil							

12.2.1	Controles contra el código malicioso		Los equipos de la compañía se encuentran protegidos por software de detección y reparación de virus y mensualmente se publican las estadísticas de virus como forma de concienciación.	Se establecerá en el documento: “Política de Seguridad de la Información” las medidas de protección frente a código malicioso			**x**	
12.3	Copias de Seguridad							
12.3.1	Copias de Seguridad de la Información		Se realizan copias de seguridad en soportes	En el documento: “Política de Seguridad de la Información” - "Resguardo de la Información" se establecerá las políticas de backup de la compañía. Se creará un instructivo Backup de servidores, donde se establecen los procedimientos para el backup diario de servidores.	**x**	**x**	**x**	**x**
12.4	Registro de actividad y supervisión.							

12.4.1	Registro y gestión de eventos de actividad.			En el documento: “Política de Seguridad de la Información” - Gestión de instalaciones externas, se especificará las políticas a tener en cuenta en caso tercerizar instalaciones de procesamiento de información. También se establecerá los Requerimientos de Seguridad en Contratos de Tercerización, con los parámetros que se deben seguir para la ejecución de este tipo de contratos.			**x**	**x**
12.4.2	Protección de los registros Información			Se establecerá que los jefes de área monitoreen y revisen regularmente los informes y registros suministrados por terceros.		**x**		
12.4.3	Registros de actividad del administrador y operador del sistema.		Se efectúan pruebas de regresión en la base de datos	Se estipula un revisión semestral de los registros de las actividades realizadas por			**x**	

				administradores y operadores del sistema.				
12.4.4	Sincronización del Reloj			En La institución de sincronizaran los relojes con el reloj de industria y comercio.	**x**		**x**	
12.5	Control del software en explotación.							
12.5.1	Instalación del software en sistemas en producción.		existe un proceso informal de aceptación de cambios en el departamento de sistemas	En el "Documento de políticas de seguridad de la información" - "Planificación y Aprobación de Sistemas" se establecerán los criterios de aprobación de nuevos sistemas de información.	**x**		**x**	
12.6	Gestión de la vulnerabilidad técnica							
12.6.1	Gestión de las vulnerabilidades técnicas.			Se establecerá el procedimiento para la gestión de vulnerabilidades en los diferentes sistemas.	**x**		**x**	
12.6.2	Restricciones en la instalación de software			En el "Documento de políticas de seguridad de la información" - "Planificación y Aprobación de Sistemas" se establecerán las	**x**		**x**	

				restricciones generales de instalación de software.				
12.7	Consideraciones de las auditorías de los sistemas de información.							
12.7.1	Controles de auditoría de los sistemas de información.			En el PSI se establecerán los controles de auditoria que la institución debe tener para los sistemas de información.	**x**		**x**	
13	**Seguridad en las Telecomunicaciones**							
13.1	Gestión de Seguridad de las Redes							
13.1.1	Controles de Red		La red de la compañía se encuentra protegida por los siguientes componentes: Firewall (prevención frente a intrusos)	Se creara el procedimiento Detección y remediación de vulnerabilidades. Se implementara sistemas de detección de intrusos.	**x**		**x**	**x**

13.1.2	Mecanismos de seguridad asociados a servicios en red.		Los nodos de acceso a la red se autentican	Se creará una norma de acceso a la red, y se incluye en los acuerdos de servicio lo enumerado en el Documento de Política de Seguridad de la Información. Seguridad Frente al Acceso por Parte de Terceros			**x**	
13.1.3	Segregación de redes.			Se estipularán los siguientes parámetros de transporte : Transporte de los equipos de cómputo Guía de entrega y recolección de correspondencia			**x**	**x**
13.2	Intercambio de información con partes externas							
13.2.1	Políticas y Procedimientos de Intercambio de Información			En el documento: “Política de Seguridad de la Información” numeral " -Acuerdos de Intercambio de Información y Software" se establecerán las políticas de intercambio de información			**x**	

13.2.2	Acuerdo de Intercambio			La organización incluirá cláusulas de confidencialidad en sus contratos con terceros		**x**	**x**	
13.2.3	Mensajería Electrónica			Las políticas de uso del correo electrónico, se encontrara publicadas en el documento: “Política de Seguridad de la Información”			**x**	**x**
13.2.4	Acuerdos de confidencialidad y secreto.			Las políticas de protección de información asociada con la interconexión, se encentrarán publicadas en el documento: “Política de Seguridad de la Información”				**x**
14	Adquisición, desarrollo y mantenimiento de sistemas de información							
14.1	Requisitos de seguridad de los sistemas							
14.1.1	Análisis y especificaciones de los requisitos de seguridad		Se conocen las leyes y contratos de seguridad de la información aplicables	En PSI - Seguridad en los Sistemas de Aplicación, se especificarán los requisitos de seguridad para los sistemas de seguridad			**x**	**x**

				En el procedimiento “Elaboración del requerimiento” se encontrarán contemplados los aspectos de seguridad como parte del proceso de desarrollo.				
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.			En el procedimiento "Autorización de retiro de información de la compañía" se especificará la autorización de retiro de información de la compañía.	**x**			**x**
14.1.3	Protección de las transacciones por redes telemáticas.			El diagnostico de vulnerabilidades se realiza de acuerdo a lo especificado en Detección y remediación de vulnerabilidades	**x**		**x**	**x**
14.2	Seguridad en los procesos de desarrollo y soporte							
14.2.1	Política de desarrollo seguro de software.			Se creara la política en el PSI - Desarrollo Seguro de Software.				

14.2.2	Procedimientos de control de cambios en los sistemas			En los procesos: Elaboración del requerimiento y Desarrollo del requerimiento. Se controlará la implantación de cambios a los sistemas de información.	**x**		**x**	
14.2.3	Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo			Se creara la política en el PSI - Revisión Técnica de los Cambios en el Sistema Operativo			**x**	
14.2.4	Restricciones a los cambios en los paquetes de software			Se creará las políticas en el PSI - Restricción del Cambio de Paquetes de Software			**x**	
14.2.5	Uso de principios de ingeniería en protección de sistemas.			En el documento PSI - Procedimiento de Control de Cambios, se definirá los siguientes controles a realizar durante la implementación del software en producción			**x**	**x**
14.2.6	Seguridad en entornos de desarrollo.		el acceso al código fuente de los programas está restringido	Se creará la política en el PSI - Control de Acceso a las	**x**		**x**	

				Bibliotecas de Programas Fuentes				
14.2.7	Externalización del Desarrollo del software			Se creará la política en el PSI - Requerimientos de Seguridad en Contratos de Tercerización	**x**			
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.			Se creará le política en el PSI - Validación de Datos de Salidas Antes de pasar a producción cualquier aplicación se deberá efectuar el procedimiento de Pruebas: Desarrollo del requerimiento			**x**	
14.2.9	Pruebas de aceptación.		existe un proceso informal de aceptación de cambios en el departamento de sistemas	En el "Documento de políticas de seguridad de la información" - "Planificación y Aprobación de Sistemas" se establecerá los criterios de aprobación de nuevos sistemas de información.	**x**		**x**	
14.3	Datos de prueba							

14.3.1	Protección de los datos utilizados en pruebas.		las pruebas se realizan en un habiente de pruebas separado	En el PSI se establecerá la Protección de los Datos de Prueba del Sistema	**x**		**x**	
15	Relaciones con Suministradores							
15.1	Seguridad de la información en las relaciones con suministradores							
15.1.1	Política de seguridad de la información para suministradores			En el documento: “Política de Seguridad de la Información” se establecerá las políticas de seguridad frente a tercerización. Se establecerá el procedimiento: Ingreso de terceros, se establecen las condiciones para permitir el ingreso de terceros a las instalaciones de la compañía.	**x**	**x**	**x**	
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.			Se levantaran matrices de Riesgo Operativo con los riesgos frente al acceso de terceros.	**x**	**x**	**x**	

15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.							
15.2	Gestión de la prestación del servicio por suministradores.							
15.2.1	Supervisión y revisión de los servicios prestados por terceros.		El departamento de sistemas actualiza los permisos de acceso cuando se entera del retiro de un funcionario	En el procedimiento "Deshabilitación de usuarios" se establecen los procedimientos de retiro de permisos para los usuarios en los sistemas de información. Cuando se presenta un cambio o retiro del cargo se deberá diligenciar el formato: "Acta de Entrega de Cargo"			**x**	**x**
15.2.2	Gestión de cambios en los servicios prestados por terceros.			En el documento: "Política de Seguridad de la Información" se establecen las políticas de seguridad frente al acceso de terceros. Numeral 2.4. En el procedimiento "MP-SOP-	**x**	**x**	**x**	

				03-02-08 Ingreso de terceros" se establecen claramente los requisitos para el ingreso de terceros a las instalaciones de la compañía				
16	Gestión de incidentes de seguridad de la información							
16.1	Gestión de Incidentes de Seguridad de la Información y Mejoras							
16.1.1	Responsabilidades y Procedimientos		Existe un procedimiento informal de registro de fallos	En el documento PSI - Procedimientos de Manejo de Incidentes se estipulará las funciones y procedimientos de manejo de incidentes, estos se encuentran descritos en el documento de Gestión de incidentes de seguridad de la información.	**x**		**x**	
16.1.2	Notificación de los Eventos de Seguridad de la Información			Establecer en el PSI políticas de Comunicación de Incidentes Relativos a la Seguridad.	**X**		**x**	

				Establecer procedimiento de: Reporte de Incidentes.				
16.1.3	Notificación de Puntos Débiles de la Seguridad			Crear en el PSI la política de Comunicación de Debilidades en Materia de Seguridad	**x**		**x**	
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.			En el documento de Política de Seguridad de la Información -Aprendiendo de los Incidentes, se estipulara el establecimiento de proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías, esta documentación de incidentes se realizará a través de: Gestión de incidentes de seguridad de la información			**x**	**x**

16.1.7	Recopilación de Evidencias			En el Documento de Política de Seguridad de la Información: Cumplimiento, se describirá los procesos de protección de registros de acuerdo a la jurisdicción relevante. Establecer el área de control interno es la encargada de efectuar las gestiones al interior de la organización para el tratamiento de evidencia frente a incidentes de seguridad de la información.	**x**		**x**	
17	Aspectos de Seguridad de la Información en la Gestión de continuidad del negocio							
17.1	Continuidad de la seguridad de la información							
17.1.1	Planificación de la continuidad de la seguridad de la información		Existe un plan de continuidad del negocio debidamente documentado	En el PSI se establecerá políticas en el Proceso de la Administración de la Continuidad de la Organización	**x**		**x**	

17.1.2	Implantación de la continuidad de la seguridad de la información		Existe un plan de recuperación de la base de datos	En el PSI se establecerá políticas de Elaboración e Implementación de los Planes de Continuidad de las Actividades de la institución	**x**		**x**	
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.			En el PSI se establecerá políticas de Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad de la organización.			**x**	
17.2	Redundancias							
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.			En el análisis de riesgos de seguridad de la información se identificaron específicamente las amenazas sobre los activos de información y el impacto de dichas amenazas para la seguridad de la información. En el PSI se establecerá la Continuidad de las Actividades y Análisis de los Impactos	**x**		**x**	

18	Cumplimiento							
18.1	Cumplimiento de los requisitos legales y contractuales							
18.1.1	Identificación de la legislación aplicable			Las leyes y normatividad aplicables a la seguridad de la información que rigen sobre la institución se encuentran documentadas en el Estatuto Orgánico.	**x**		**x**	
18.1.2	Derechos de Propiedad Intelectual (DPI)		los derechos de propiedad intelectual son contemplados en los acuerdos de servicios	En el PSI se establecerá los Derechos de Propiedad Intelectual, la institución deberá contar con un software que permite detectar el uso de software no autorizado en la institución.	**x**	**x**	**x**	

18.1.3	Protección de los registros de la Organización		Existe un área de archivo en donde se custodian los registros importantes de la institución.	En el PSI se establecerá la Protección de los Registros de la organización En el proceso “Creación e ingreso de garantías al sistema” se estipulará del proceso para el correcto archivo de garantías y en el “ Préstamo de garantías” se establece el procedimiento de préstamo. El único departamento autorizado para solicitar garantías será el departamento financiero. -El encargado del área de archivo cuenta con una lista de personas autorizadas para el préstamo de carpetas. El uso de esta lista se encuentra registrado en los procesos “Solicitud de carpetas en el archivo” y	**x**	**x**	**x**	

				"Creación de carpetas en el archivo"				
18.1.4	Protección de Datos y privacidad de la información personal			Se creará en el PSI - Protección de Datos y Privacidad de la Información Personal, se establecerá una definición de la responsabilidad del manejo de los datos de carácter personal.	**x**		**x**	
18.1.5	Regulación de los Controles Criptográficos		Se conocen y cumplen los requisitos emitidos por los entes de control sobre los controles cifrados.	Se creará en el PSI la sección Regulación de Controles	**x**		**x**	

18.2	Revisiones de la seguridad de la información.							
18.2.1	Revisión independiente de la seguridad de la información.			En el PSI - Revisión de Derechos de Acceso de Usuarios, se establecerá la creación de un perfil especial para la función de auditoría		**x**		
18.2.2	Cumplimiento de las políticas y normas de seguridad		Existe un acuerdo de confidencialidad en los contratos laborales	Crear el procedimiento "Selección de proveedores" y el procedimiento "Compras", se establece la firma por parte del proveedor de un acuerdo de confidencialidad diseñado y aprobado por el departamento jurídico de la compañía.	**x**	**x**	**x**	
18.2.3	Comprobación del cumplimiento.			Agregar en el PSI - Verificación de la Compatibilidad Técnica		**x**	**x**	

Cuadro 22: Declaración de Aplicabilidad

ANEXO XII

INFORME DE AUDITORIA DE CUMPLIMIENTO

Nivel de Madurez CMM para los dominios de la norma

ISO/IEC 27001:2013

Elaborado por: Luis Fernando Echeverría

diciembre 2017

Contenido

AUDITORIA DE CUMPLIMIENTO

I RESUMEN EJECUTIVO

Alcance

Auditoría del Sistema de Gestión de la Seguridad de la institución dentro de los límites del alcance del SGSI y de la declaración de aplicabilidad de los diferentes controles.

Objetivo

Evaluar la madurez de la Seguridad en lo que respecta a los diferentes dominios de control los 114 controles planteados por la ISO/IEC 27002:2013.

Metodología

El proceso de auditoría de cumplimiento se la ha realizado mediante una evaluación al cumplimiento de cada uno de los controles de la norma ISO / IEC 27002: 2013, para ello se ha utilizado el Modelo de Madurez de la Capacidad (CMM). Esta evaluación de control se la ha realizado mediante un análisis de los recursos que se disponen: documentación existente dentro de la institución, reportes de

evidencias, reportes de incidentes, reportes de funcionamiento de la institución, de reportes de evaluaciones, reportes de auditorías precedentes, reportes de entrevistas, de tests y observaciones realizadas in situ.

Principales conclusiones

Al ser una entidad nueva su nivel de madurez no es el óptimo, por lo que existe varias inconformidades. Los resultados obtenidos en los diferentes dominios muestran que la institución tiene un bajo consciente de la importancia de la seguridad de la información y para ello se debe implementar medidas tanto funcionales como técnicas que permitan mejorar el manejo seguro de la información.

La auditoría ha permitido identificar 22 no conformidades de las cuales 5 conformidades mayores. Resultado de estos hallazgos se constata que existen deficiencias menores en las medidas que se han tomado para controlar los accesos a la información y a los recursos de manejo de la información, no obstante, se tiene varios controles que mejorar.

Se han identificado que existen deficiencias en la concientización de los usuarios afectando de manera directa el nivel de seguridad del manejo de la información.

Recomendaciones

Es necesario tomar acciones inmediatas para subsanar primero las no conformidades mayores planificando la conclusión de la mismas en un periodo de tiempo corto, lo que permitiría mejorar el nivel de la seguridad en un plazo corto. Si

bien no existe un plazo límite para tomar acciones para subsanar las no conformidades menores, es recomendable una planificación inmediata de ejecución de las mismas.

II METODOLOGIA

El proceso de auditoría de cumplimiento se la ha realizado mediante una evaluación al cumplimiento de cada uno de los controles de la norma ISO / IEC 27002: 2013, para ello se ha utilizado el Modelo de Madurez de la Capacidad (CMM).

Fases de la Auditoria

Fase 1: Recolección de la Información

Durante esta etapa se ha solicitado toda la documentación relevante al proceso de auditoría. documentación que permite entender el entorno del ambiente a auditar, las políticas, los procedimientos definidos, los procesos implementados, los registros e informes y evaluaciones precedentes, etc.

Es en esta etapa que se realiza la identificación y la asignación de recursos.

Fase 2. Ejecución de pruebas documentadas

Revisión de la documentación que se ha recopilado con el fin de comprobar la idoneidad y relevancia con el proceso de auditoría que se lleva a cabo.

Se han revisado y validado el estado de implementación de los procedimientos y procesos Asociados al manejo de la información y los sistemas de información.

Se verifica la implementación de los distintos controles estipulados en la declaración de la aplicabilidad.

Se han procedido a entrevistas para comprobar si el personal de la institución conoce las políticas, procesos y procedimientos y las aplica.

Se han realizado visitas para examinar aspectos de seguridad y comprobar in situ el modo en el que maneja la información y se operan los sistemas de información.

Fase3: Análisis de la información

Se ha analizado toda la documentación disponible y las evidencias que se han recolectado para poder determinar el nivel de cumplimiento con la norma.

Esta fase se ha enfocado por un lado en la revisión de las políticas, para verificar que se encuentran al alcance del personal, que son claras, relevantes, que protegen los activos identificados, que se conocen a los responsables de emitir estas políticas y a quienes afectan las mismas. Po otro lado se enfoca en el análisis de los resultados de las entrevistas, de las verificaciones y observaciones que se han realizado en situ y así poder evaluar si las políticas se distribuyen, se comunican y se aplican. Es a partir de este análisis que se puede concluir la efectividad de los controles implementados.

Como resultado de esta fase se han identificado los incumplimientos a la norma y muestra la eficiencia y la efectividad de los controles de seguridad.

Fase 4: Elaboración y presentación del Reporte de la Auditoria

Se elabora el informe de auditoría que transmite las conclusiones a las que se han llegado.

III HALLAZGOS y RECOMENDACIONES

Puntos Fuertes

• COMPROMISO POR PARTE DE LA DIRECCION

Se constata que la Dirección está consciente y realmente comprometida con la implementación del PLAN SGSI.

• POLITICAS DEFINIDAS

El documento de las políticas, están definidas, está pendiente de aprobación por parte de la dirección. De igual manera se han dado los instructivos provenientes de la dirección para que estos sean comunicados a todos los estudiantes, docentes y personal administrativo de la institución.

Oportunidades de mejora

• FORMACION/CONCIENTIZACION

Si bien la institución tiene planificado un plan de formación para todos los miembros de la institución (estudiantes, docentes y personal administrativo), este plan de

formación es obligatorio por lo menos una vez al año y cada vez que el usuario cambia de puesto de trabajo.

Se han identificado en algunos miembros del personal cierta desactualización en algunos temas relacionado al manejo de la seguridad. Es por eso que se plantea que el personal de la institución debería pasar por el proceso de concientización/formación por lo menos una vez al año. Para dar mayor flexibilidad y accesibilidad a la formación se podría considerar implementar una metodología de e-learning.

No Conformidades

ID: NC-001	**Fecha: 04/12/2017**
Descripción NC	
En la institución cuentan con un borrador de políticas de seguridad la misma que no está revisada, aprobada, publicada y comunicada.	
Tipo **Mayor X** **Menor**	
Referencia normativa	
Controles	**Dominio**
5.1.1 Políticas para la seguridad de la información	5.1 Directrices de la Dirección en seguridad de la información
Acción Correctora	
• Se debe definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes.	
Responsable Ejecución acción correctora	
El responsable de la seguridad con aprobación de la Dirección	

ID: NC-002	**Fecha: 04/12/2017**

Descripción NC		
En la institución realiza la investigación de antecedentes en un bajo nivel, no cuenta con un check list, los contratos laborales cuenta con los términos y condiciones en un alto porcentaje con docentes y personal administrativo no así con los contratistas y terceros.		
Tipo	**Mayor**	**Menor X**
Referencia normativa		
Controles	**Dominio**	
7.1.1 Investigación de antecedentes 7.1.2 Términos y condiciones de contratación	7.1 Antes de la contratación	
Acción Correctora		
• Se debe realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. • Como parte de su obligación contractual, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.		
Responsable Ejecución acción correctora		
El responsable de Talento Humano y Administradores de Contrato		

ID: NC-003	**Fecha: 04/12/2017**
Descripción NC	
En la institución cuenta con un listado de contratistas y usuarios de terceros no se aplica la seguridad de acuerdo a lo establecido en las políticas y procedimientos. En el último año no se ha procedido un entrenamiento en conocimiento y actualizaciones regulares en políticas y procedimientos. No se tiene establecido sanciones de acuerdo a los niveles de criticidad.	
Tipo **Mayor** **Menor X**	

Referencia normativa	
Controles	**Dominio**
7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en SI. 7.2.3 Proceso disciplinario.	7.2 Durante la contratación

Acción Correctora

- La Dirección debe requerir a contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos.
- Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.
- Debe existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.

Responsable Ejecución acción correctora

El responsable de Talento Humano y responsable de la seguridad.

ID: NC-004	**Fecha: 04/12/2017**

Descripción NC

La institución cuenta con un procedimiento informal de salida de personal administrativo, docentes y estudiantes, los mismo cuenta con un formulario de salida en donde es firmado por las principales áreas indicando si tiene algún pendiente, el ultimo registró es la Dir. de TICs, en donde procede con la baja del usuario.

Tipo **Mayor** **Menor X**

Referencia normativa	
Controles	**Dominio**
7.3.1 Cese o cambio de puesto de trabajo	7.3 Cese o cambio de puesto de trabajo

Acción Correctora

- Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.

Responsable Ejecución acción correctora
El responsable de Talento Humano

ID: NC-005	**Fecha: 04/12/2017**
Descripción NC	
La institución tiene un control de activos los mismos que se encuentran catalogados, algunos activos de TI no se están registrador el número de serie. Se asigna los activos a cada miembro de la institución, no es así con personal con contrato de servicio ocasional. El procedimiento de devolución de activos en algunos casos lo realizan después de que ya salió el personal.	
Tipo **Mayor** **Menor X**	
Referencia normativa	
Controles	**Dominio**
8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos.	8.1 Responsabilidad sobre los activos
Acción Correctora	
• Todos los activos deben estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes. • Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización. • Se debe identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información. • Todos los empleados y usuarios de terceras partes deben devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.	
Responsable Ejecución acción correctora	

El responsable de Talento Humano

ID: NC-006	**Fecha: 04/12/2017**
Descripción NC	
Existe procedimientos operativos pobres para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas. Se adoptado un sistema que cifra los datos sensibles o valiosos antes de ser transportados.	
Tipo **Mayor** **Menor X**	
Referencia normativa	
Controles	**Dominio**
8.3.1 Gestión de soportes extraíbles: 8.3.2 Eliminación de soportes: 8.3.3 Soportes físicos en tránsito:	8.3 Manejo de los soportes de almacenamiento
Acción Correctora	
• Se debe establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización. • Se deber eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales. • Se debe proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.	
Responsable Ejecución acción correctora	
El responsable Dirección de TI.	

ID: NC-007	**Fecha: 04/12/2017**
Descripción NC	

Existe un procedimiento informal para el aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso, esto se realiza cuando Talento Humano emite un correo solicitando la creación de usuarios. Los propietarios de los activos no realizan una revisión periódica de los derechos de acceso de los usuarios. Para retirar o cambios de los derechos de acceso de los usuarios también es enviado via correo electrónico por Talento Humano, pero este no llega con la inmediata salida del funcionario si no cada fin de mes.	
Tipo **Mayor** **Menor X**	
Referencia normativa	
Controles	**Dominio**
9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios 9.2.6 Retirada o adaptación de los derechos de acceso	9.2 Gestión de acceso de usuario
Acción Correctora	
• Se debe implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios. • Los propietarios de los activos deben revisar con regularidad los derechos de acceso de los usuarios. • Se debe retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.	
Responsable Ejecución acción correctora	
El responsable Dirección de TI.	

ID: NC-008	**Fecha: 04/12/2017**
Descripción NC	

Existe acceso a los servidores de forma remota de forma segura con llaves criptográficas, no se ha establecido un ciclo de vida de dichas contraseñas, esto también no está estipulado formalmente.		
Tipo	**Mayor**	**Menor X**
Referencia normativa		
Controles		**Dominio**
10.1.2 Gestión de claves.		10.1 Controles criptográficos
Acción Correctora		
• Se debe desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.		
Responsable Ejecución acción correctora		
El responsable Dirección de TI.		

ID: NC-009	**Fecha: 04/12/2017**
Descripción NC	
La institución ha mantenido una política de disponibilidad de activos y equipos para los docentes y no se ha planteado controles para proteger la información que se encuentra almacenada dentro de estas.	

Tipo	**Mayor**	**Menor X**
Referencia normativa		
Controles		**Dominio**
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario		11.2 Seguridad de los equipos
Acción Correctora		

- Se debe aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.
- Se debe verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.
- Los usuarios deben asegurar de que los equipos no supervisados cuentan con la protección adecuada.

Responsable Ejecución acción correctora
El responsable Dirección de TI.

ID: NC-010	**Fecha: 04/12/2017**
Descripción NC	
Debido a que la institución es nueva y está en un crecimiento ascendente varios cambios han afectado la seguridad de la información, lo que se ha mantenido son las instalaciones. La proyección de los recursos se han establecido de acuerdo a las necesidades institucionales, no existe un marco de trabajo definido.	
Tipo **Mayor** **Menor X**	
Referencia normativa	
Controles	**Dominio**
12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades.	12.1 Responsabilidades y procedimientos de operación
Acción Correctora	

- Se debe controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.
- Se debe monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

Responsable Ejecución acción correctora
El responsable Dirección de TI.

ID: NC-011	**Fecha: 04/12/2017**
Descripción NC	
Actualmente la institución tiene relación con dos principales organizaciones como son: Yachay E.P. y EPICentro; para lo cual intercambian información sensible pero no adoptado las medidas de seguridad necesaria.	
Tipo **Mayor** **Menor X**	
Referencia normativa	
Controles	**Dominio**
13.2.2 Acuerdos de intercambio	13.2 Intercambio de información con partes externas
Acción Correctora	
• Establecer acuerdos donde se aborde la transferencia segura de información comercial entre la organización y las partes externas.	
Responsable Ejecución acción correctora	
El responsable Dirección de TI.	

ID: NC-012	**Fecha: 04/12/2017**
Descripción NC	
Actualmente existe un área de desarrollo que realiza el levantamiento de información y asigna los accesos correspondientes al sistema, no se tiene un análisis adecuado de los requisitos de seguridad del sistema esto debe formalizarse.	
Tipo **Mayor** **Menor X**	
Referencia normativa	
Controles	**Dominio**
14.1.1 Análisis y especificación de los requisitos de seguridad 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	14.1 Requisitos de seguridad de los sistemas de información
Acción Correctora	

• Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes. • La información de los servicios de aplicación que pasan a través de redes públicas se deberían proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.
Responsable Ejecución acción correctora
El responsable Dirección de TI.

ID: NC-013	**Fecha: 04/12/2017**
Descripción NC	
Actualmente no se tiene políticas de desarrollo formalizadas, existe procedimientos informales para el control de cambios en los sistemas. El sistema de gestión académica cuenta con un ambiente de pruebas en el mismo se realiza actividades operativas antes de entrar a producción.	
Tipo **Mayor** **Menor X**	
Referencia normativa	
Controles	**Dominio**

14.2.1 Política de desarrollo seguro de software 14.2.2 Procedimientos de control de cambios en los sistemas 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software. 14.2.5 Uso de principios de ingeniería en protección de sistemas 14.2.6 Seguridad en entornos de desarrollo 14.2.7 Externalización del desarrollo de software	14.2 Seguridad en los procesos de desarrollo y soporte
Acción Correctora	

• Se debe establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización. • En el ciclo de vida de desarrollo se debe hacer uso de procedimientos formales de control de cambios. • Las aplicaciones críticas para el negocio se deben revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización. • Se debe evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todo el cambio se debe controlar estrictamente. • Se debe establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información. • La organización debe establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema. • La organización debe supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado. • Se debe realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
Responsable Ejecución acción correctora
El responsable Dirección de TI.

ID: NC-014	**Fecha: 04/12/2017**
Descripción NC	
Actualmente la institución está trabajando en un plana de continuidad del negocio en donde se contempla temas de seguridad.	
Tipo **Mayor** **Menor X**	
Referencia normativa	
Controles	**Dominio**

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	17.1 Continuidad de la seguridad de la información
Acción Correctora	
• La organización debe verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.	
Responsable Ejecución acción correctora	
El responsable Dirección de TI.	

ID: NC-015	**Fecha: 04/12/2017**	
Descripción NC		
Actualmente el data center local cuenta con un TIER I, y se encuentran en proceso de mejora para subir a un TIER II, respecto al enlace de datos con el IaaS se tiene una disponibilidad del 98,6%.		
Tipo	**Mayor**	**Menor X**
Referencia normativa		
Controles		**Dominio**
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.		17.2 Redundancias
Acción Correctora		
• Se debe implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.		
Responsable Ejecución acción correctora		
El responsable Dirección de TI.		

ID: NC-016	**Fecha: 04/12/2017**
Descripción NC	

El estado ecuatoriano a través de una nueva normativa establece que todo software desarrollado por una entidad pública le pertenece al estado, por lo que no está establecido es un procedimiento formal para el registro del código fuente. Actualmente se esta estableciendo los mejores métodos de encriptación para el almacenamiento de ciertos datos sensibles.

Tipo	**Mayor**	**Menor X**

Referencia normativa	
Controles	**Dominio**
18.1.2 Derechos de propiedad intelectual (DPI) 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	18.1 Cumplimiento de los requisitos legales y contractuales

Acción Correctora

- Se debe implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales.
- Los registros se deben proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.
- Se debe utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

Responsable Ejecución acción correctora
El responsable Dirección de TI.

ID: NC-017	**Fecha: 04/12/2017**

Descripción NC
La institución tiene planificado establecer un plan de seguridad de la información y mantener una auditoria de certificación para el año 2019.

Se establece un comité de seguridad el mismo que no estipula funciones claras para su actividad.	
Tipo **Mayor** **Menor X**	
Referencia normativa	
Controles	**Dominio**
18.2.1 Revisión independiente de la seguridad de la información 18.2.2 Cumplimiento de las políticas y normas de seguridad 18.2.3 Comprobación del cumplimiento	18.2 Revisiones de la seguridad de la información
Acción Correctora	
• Se debe revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización. • Los gerentes deben revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente. • Los sistemas de información se debe revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización	
Responsable Ejecución acción correctora	
El responsable Dirección de TI.	

ID: NC-018	**Fecha: 04/12/2017**
Descripción NC	

En la institución cuentan con plataforma de TI Windows y Linux, se tiene servicios de seguridad como antivirus, firewall, entre otras, no se tiene evidencia de mantener contacto con grupos o foros de seguridad especializados y asociaciones profesionales, no se tiene actividades proactivas que ayuden a prevenir posibles riesgos de seguridad.	
Tipo **Mayor X** **Menor**	
Referencia normativa	
Controles	**Dominio**
6.1.4 Contacto con Grupos de Interés Especial	6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
Acción Correctora	
• Definir grupos de interés de acuerdo a la plataforma tecnológica y servicios de TI que son ofrecidos a los estudiantes, docentes y personal administrativo. Por ejemplo: grupos independientes de evaluación de antivirus, centro de descargas de soluciones de Microsoft, grupos de información actualizada sobre amenazas de Internet que estén activas, etc.	
Responsable Ejecución acción correctora	
El responsable de la seguridad con aprobación de la Dirección	
ID: NC-019 Fecha: 04/12/2017	
Descripción NC	
La institución tiene tres plataformas de TI que son: Windows, Linux y MAC; al igual	
Tipo Mayor X Menor	
Referencia normativa	
Controles Dominio	
12.6.1 Gestión de las vulnerabilidades técnicas	12.6 Gestión de la vulnerabilidad técnica
Acción Correctora	
• Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.	
Responsable Ejecución acción correctora	
Responsable Administradores de Contrato y Dirección de TI	

ID: NC-020 Fecha: 04/12/2017	
Descripción NC	
La institución no cuenta con área de auditoria, al igual no se conocimiento si se tiene planificado contratar una auditoria externa cuya finalidad sea auditor los sistemas de información en donde se debe identificar la existencia de controles para salvaguardar los sistemas operacionales y herramientas de auditoría.	
Tipo	**Mayor X** **Menor**
Referencia normativa	
Controles Dominio	
12.7.1 Controles de auditoría de los sistemas de información.	12.7 Consideraciones de las auditorías de los sistemas de información
Acción Correctora	
• Se debe planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.	
Responsable Ejecución acción correctora	
Responsable Alta dirección y Dirección de TI	

ID: NC-021 Fecha: 04/12/2017	
Descripción NC	
Actualmente la institución cuenta con una data center en donde se realiza parte del procesamiento de información. al mismo se tiene registros que ingresan personal que no es de la institución por dos razones concretas: Mantenimiento de dispositivos electrónicos y eléctricos. Mantenimiento de la conexión de la red WAN. Al igual se tiene contratado IaaS y SaaS contratados con proveedores externos a los cuales se tiene un contrato con SLAs, pero no se tiene cláusulas de confidencialidad	
Tipo	**Mayor X** **Menor**
Referencia normativa	
Controles Dominio	

15.1.1 Política de seguridad de la información para suministradores. 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	15.1 Seguridad de la información en las relaciones con suministradores.

Acción Correctora

- Se debe acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.
- Se debe establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización.
- Se debe establecer acuerdos con los proveedores en donde se incluya los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

Responsable Ejecución acción correctora

Responsable Administradores de Contrato y Dirección de TI

ID: NC-022 Fecha: 04/12/2017		
Descripción NC		
Actualmente la institución no tiene definido formalmente las funciones y procedimientos para gestionar los incidentes de seguridad de la información, por lo que no cuenta con notificaciones de eventos y puntos débiles de seguridad, tampoco con la valoración y respuesta a incidentes.		
Tipo	**Mayor X**	**Menor**
Referencia normativa		
Controles Dominio		

16.1.1 Responsabilidades y procedimientos 16.1.2 Notificación de los eventos de seguridad de la información 16.1.3 Notificación de puntos débiles de la seguridad 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones 16.1.5 Respuesta a los incidentes de seguridad 16.1.6 Aprendizaje de los incidentes de seguridad de la información	16.1 Gestión de incidentes de seguridad de la información y mejoras

Acción Correctora

- Se debe establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
- Los eventos de seguridad de la información se deben informar lo antes posible para lo cual se debe establecer los canales de administración adecuados.
- Se debe requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios los estudiantes, docentes y personal administrativo como a contratistas que utilizan los sistemas y servicios de información de la organización.
- Se debe evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.
- Se debe responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.
- Se debe utilizar el conocimiento obtenido el análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.
- La organización debe definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

Responsable Ejecución acción correctora

Responsable	Alta dirección y Dirección de TI

IV CONCLUSIONES

Los resultados confirman que la institución en su totalidad participa en la implementación de los controles necesarios para garantizar un manejo seguro de la información. Si bien no se ha llegado al nivel objetivo y existen no conformidades mayores y menores, los resultados obtenidos en los diferentes dominios muestran que la institución es consciente de la importancia de la seguridad de la información y para ello ha implementado medidas tanto funcionales como técnicas que permiten mejorar el manejo seguro de la información.

El resultado de la evaluación del nivel de madurez de seguridad de la información en la institución no es satisfactorio puesto que menos de la mitad de procesos y controles se encuentran en el nivel “Proceso definido”.

Los resultados muestran que a través de la implementación de este plan director se están consiguiendo mejoras sustanciales en los diferentes dominios de la norma de referencia.

9 Bibliografía

- MATERIAL UOC

  Asignatura Sistemas de Gestión de la Seguridad

  Modulo 1: Introducción a la Seguridad de la Información

  Modulo 2: Análisis de riesgos

  Modulo 3: Implantación de un Sistema de Gestión de la Seguridad de la Información

  Modulo 4: Desarrollo de Algunos Objetivos de control del SGSI

  Asignatura de la Auditoria

  Modulo 2: Auditoria de Certificación
- ISO 27001: Revisión por la dirección y mejora del SGSI

  http://www.pmg-ssi.com/2014/12/iso-27001-revision-por-la-direccion-ymejora-del-sgsi/
- ¿Qué es el Capability Maturity Model (CMM®)?

  http://www.pmvalue.com.ar/newsletters/Newsletter%20-%20CMM.pdf
- MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
- El portal de ISO 27001 en Español. Gestión de Seguridad de la Información.

  http://www.iso27000.es/iso27000.html
- Esquema Gubernamental de Seguridad de la Información (EGSI). Modelo de Seguridad
- http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%83%C2%B3n.pdf
- ENISA – European Union Agency for Network and Information Security

  https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment
- Estructura Orgánica de la Institución https://www.yachaytech.edu.ec/wp-content/uploads/2017/08/a1-organigrama-de-la-institucion-JULIO2017.pdf
- Sistema de información pública de la Institución https://sites.google.com/yachaytech.edu.ec/infor/inicio
- Base Legal que rige a las Instituciones Públicas https://www.yachaytech.edu.ec/wp-content/uploads/2017/08/a2-base-legal-que-rige-a-la-institucion-JULIO2017.pdf
- Estatuto Organico de la Institución https://yachaytech.edu.ec/fileadmin/user_upload/uploads/LOTAIP-2017/FEBRERO/a1Estatutocodificado/a1.-ESTATUTO_YT_CODIFICADO.pdf