Propuesta de Implementación de un SGSI basado en la Norma ISO 27001.
(Caso práctico Universidad de El Salvador).

Cazco Rafael, Galindo Ellen, Nóchez Tanya
UNIVERSIDAD DON BOSCO
ANTIGUO CUSCATLAN, EL SALVADOR
rafa.cazco@gmail.com
ellengraciela@gmail.com
tnochez@gmail.com

Resumen—

La Universidad de El Salvador (UES) fue fundada el 16 de Febrero de 1841, es la única Universidad pública en el país y tiene presencia en varios departamentos del territorio Salvadoreño.

Debido a que la información es uno de los activos más importantes para la UES (y cualquier organización hoy en día), se vuelve crítico asegurar la integridad, disponibilidad y confidencialidad de la misma.

Para lograr lo anterior se realizó un análisis del estado actual de la UES en relación a la gestión de la seguridad de la información, el cual sirve como insumo para la propuesta de implementación de un SGSI basado en la norma ISO 27001:2005.

Índice de Términos—SGSI, ISO, Confidencialidad, Disponibilidad, Integridad, Riesgo de TI.

I. INTRODUCCIÓN

En la actualidad, la información, junto a los procesos y sistemas que hacen uso de ella son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible son esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial, por lo que se debe mantener una adecuada seguridad en la información utilizada en la organización. Todo lo mencionado es necesario para lograr a cumplir los objetivos estratégicos de la organización y asegurar beneficios económicos.

Es por lo anterior que, en el estudio realizado a la UES, sobre la propuesta de implementación de un SGSI basado en la Norma 27001, se consideraron los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente originándose dentro de la propia organización o aquellos provocados por catástrofes naturales y fallas técnicas.

La UES, alberga a más de 53,000 estudiantes entre sus cuatro campus localizados en San Salvador (Ciudad Universitaria – campus principal), Santa Ana, San Miguel y San Vicente. Ofrece 169 carreras divididas en doce facultades.

El ranking mundial de Universidades en la Web, realizado por el CSIC (Consejo Superior de Investigaciones Científicas) clasifica a la UES como la mejor universidad de la república, a nivel internacional se encuentra en el puesto 3393.

Por lo anterior, se establece que el cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos del negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de la UES.

II. SITUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Se analizó la información sobre la situación actual de la seguridad de la información en la UES, encontrando algunos puntos importantes sobre la

gestión de la seguridad de la información, los cuales se detallan a continuación:

Fortalezas:
• Las aperturas a nuevos cambios para la propuesta de implementación del SGSI.

Oportunidades:
• Múltiples centros de datos con redundancia.

Debilidades:
• Actualmente, la UES no cuenta con un área o departamento dedicado a la gestión de la Seguridad de la información, por tanto cada área de IT (Infraestructura, telecomunicaciones, Desarrollo, etc.) tiene sus propias metodologías y procedimientos para velar por la seguridad de la información.

• No se posee un sistema centralizado que sea utilizado por todas las facultades. Cada facultad tiene sistemas independientes para realizar los procesos de índole académico y administrativos.

• No cuentan con un SGSI documentado, ni políticas de seguridad definidas ni divulgadas. Algunas áreas cuentan con procedimientos pero no están centralizados y no se les da un cumplimiento constante.

• No poseen interfaces de forma automática entre las aplicaciones funcionando en la UES, lo que permite crear procesos innecesarios para manejar la información.

• No existen controles para el acceso físico a la infraestructura que almacena los activos de información, ni hay bitácoras de acceso, ni procedimientos de revisión de las mismas.

• Cuenta con un control de acceso deficiente.

Amenazas:
• No realizan auditorías periódicas de los sistemas de la UES.

Adicional, se solicitó a la UES realizar una autoevaluación en diferentes elementos de seguridad, obteniendo los siguientes resultados:

Políticas de Seguridad

Pregunta autoevaluación	Resultado (SI/NO)
Existencia de documentos de política de seguridad	NO
Existencia de normativa relativa a la seguridad de los sistemas de información.	NO
Existencia de procedimientos relativos a la seguridad de la información.	NO
Existencia de responsables, mecanismos de comunicación y controles para verificar la efectividad de las políticas	NO

(Tabla 1 – Políticas de Seguridad).

Administración de activos

Pregunta autoevaluación	Resultado (SI/NO)
Inventario de activos actualizado.	SI
Existencia de un responsable de los activos.	SI
Existencia de procedimientos para clasificación y etiquetado de la información.	NO

(Tabla 2 – Administración de activos).

Organización de la seguridad

Pregunta autoevaluación	Resultado (SI/NO)
Existencia de roles y responsabilidades definidas	NO

Existencia de criterios de seguridad en el manejo de terceras partes.	NO
Existencia de programas de formación en seguridad para empleados, clientes y otros.	NO
Existencia de un buen acuerdo de confidencialidad.	NO

(Tabla 3 – Organización de la Seguridad).

Seguridad de los RRHH

Pregunta autoevaluación	Resultado (SI/NO)
Consideración de la seguridad en la selección y baja del personal	NO
Imposición de los condicionantes de confidencialidad y responsabilidad en los contratos	SI

(Tabla 4 – Seguridad de los RRHH).

Seguridad Física y del Ambiente

Pregunta autoevaluación	Resultado (SI/NO)
Existencia de protecciones frente a fallos en la alimentación eléctrica.	SI
Garantía de disponibilidad e integridad de todos los equipos.	SI

(Tabla 5 – Seguridad Física y del Ambiente).

Gestión de comunicaciones y operaciones

Pregunta autoevaluación	Resultado (SI/NO)
Existencia de controles en la redes.	SI
Establecimiento de medidas para proteger la confidencialidad e integridad de la información publicada.	SI
Monitoreo de las actividades relacionadas con la seguridad.	NO

(Tabla 6 – Gestión de Comunicaciones y Operaciones).

Control de acceso

Pregunta autoevaluación	Resultado (SI/NO)
Control y restricción de la asignación y uso de privilegios en entornos multiusos	NO
Incorporación de medidas de seguridad en computadoras móviles.	NO
Garantía de la seguridad de la ruta desde el terminal al servicio	NO

(Tabla 7 – Control de Acceso).

Desarrollo y mantenimiento de los sistemas

Pregunta autoevaluación	Resultado (SI/NO)
Existencia de controles criptográficos.	SI
Seguridad en los ficheros de los sistemas	NO
Control de las vulnerabilidades de los equipos.	NO

(Tabla 8 – Desarrollo y mantenimiento de los sistemas).

Administración de incidentes

Pregunta autoevaluación	Resultado (SI/NO)
Comunicación de los eventos de seguridad.	SI
Comunicación de las debilidades de seguridad.	SI
Definición de responsabilidades ante un incidente	SI

(Tabla 9 – Administración de incidentes).

Gestión de la continuidad del negocio

Pregunta autoevaluación	Resultado (SI/NO)
Existencia de un plan de continuidad del negocio y análisis de impactos.	NO
Existencia de procesos para la gestión de la continuidad.	NO

(Tabla 10 – Gestión de la continuidad del negocio).

III. ENTORNO TEÓRICO

A. Seguridad de la Información

La seguridad de la información es la preservación de los principios básicos de la confidencialidad, integridad y disponibilidad de la misma y de los sistemas implicados en su tratamiento. Estos tres pilares se definen como:

• Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.

• Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

En la seguridad de la información, no solo intervienen los aspectos tecnológicos, sino también los procesos, los ambientes (centro de cómputo, ubicación de oficinas) y principalmente las personas.

B. ISO

La ISO desarrolla estándares requeridos por el mercado que representan un consenso de sus miembros acerca de productos, tecnologías, sistemas y métodos de gestión, entre otros. Estos estándares, por naturaleza, son de aplicación voluntaria, ya que el carácter no gubernamental de ISO no le da autoridad legal para forzar su implantación. Sólo en aquellos casos en los que un país ha decidido adoptar un determinado estándar como parte de su legislación, puede convertirse en obligatorio.

C. NORMA ISO 27001:2005

Es un estándar ISO que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en el ciclo de vida PDCA (Planear-Hacer-Verificar-Actuar) de mejora continua, al igual que otras normas de sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

D. Serie ISO27000

ISO ha reservado la serie de numeración 27000 para normas relacionadas con sistemas de gestión de seguridad de la información. En 2005 incluyó en ella la primera de la serie (ISO 27001), las demás son:

• ISO27000 (términos y definiciones),
• ISO27002 (objetivos de control y controles),
• ISO27003 (guía de implantación de un SGSI),
• ISO27004 (métricas y técnicas de medida de la efectividad de un SGSI),
• ISO27005 (guía para la gestión del riesgo de seguridad de la información) y
• ISO27006 (proceso de acreditación de entidades de certificación y el registro de SGSI).

E. NORMA ISO27003

ISO-27003 focaliza su atención en los aspectos requeridos para un diseño exitoso y una buena implementación del Sistema de Gestión de Seguridad de la Información – SGSI – según el estándar ISO 27001.

F. SGSI

Un SGSI es un Sistema de Gestión de la Seguridad de la Información o ISMS por sus siglas en inglés (Information Security Management System). Este sistema consiste de una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por una organización o entidad.

El propósito de un sistema de gestión de la seguridad de la información no es garantizar la seguridad – que nunca podrá ser absoluta- sino garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.

IV. PLANTEAMIENTO DEL PROBLEMA

Actualmente la UES no cuenta con un área o departamento dedicado a la gestión de la Seguridad de la información, por tanto cada área de IT (Infraestructura, telecomunicaciones, Desarrollo, etc.) tiene sus propias metodologías y procedimientos para velar por la seguridad de la información.

Tampoco cuentan con un SGSI documentado, ni políticas de seguridad definidas ni divulgadas. Algunas áreas cuentan con procedimientos pero no están centralizados y no se les da un cumplimiento constante.

Por estos motivos es muy importante que la UES implemente el SGSI planteado para fortalecer los controles que aseguren la disponibilidad, confidencialidad e integridad de la información de la UES. Y para administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables teniendo en cuenta la clasificación de los riesgos e incrementar la capacidad, el desarrollo y buen uso de las tecnologías de información y comunicación en la UES.

V. SOLUCIÓN PLANTEADA

A. Política de seguridad de la información

1. Objetivos

1.1 Objetivos Generales.

- Proteger la Integridad, Disponibilidad y Confidencialidad de la información y sistemas de información de la UES.
- Definir la base para aplicar controles, procedimientos y/o estándares relacionados con la seguridad de la información.
- Establecer las normas de seguridad de la información de la UES y regular la gestión de la misma al interior de la UES.

1.2 Objetivos Específicos.

- Definir y comunicar la responsabilidad del uso de los activos de información que soportan los procesos y sistemas de la UES.
- Proteger la imagen, intereses y reputación de la UES a través de una adecuada gestión de la seguridad de su información.
- Definir las conductas permitidas referentes al acceso, uso, manejo y administración de los recursos de información.
- Establecer los canales de comunicación que le permitan al Concejo Superior Universitario de la UES mantenerse informado de los riesgos, incidentes y uso inadecuado de los activos de información, y de las acciones tomadas para su mitigación y corrección.

2. Alcance

La presente política aplica para toda información propia de la UES, o de Colaboradores/Terceros bajo la responsabilidad de la UES, que sea creada, procesada o utilizada como parte del soporte a la UES; independiente del formato, medio,

presentación y/o ubicación. Dicha política es aplicable a todos los campus en El Salvador.

Todos los Colaboradores y Terceros están obligados a conocer, cumplir y hacer cumplir su responsabilidad respecto a los riesgos en el manejo de los activos de información de la UES.

La gestión de la seguridad es una actividad propia de la UES y no puede ser ejecutada por personal ajeno a la UES o terceras personas sin previa autorización.

3. Responsables de implementación.

La Unidad de Gestión de Sistemas de Información y Telecomunicaciones es la responsable de generar la Política y mantenerla actualizada, además es responsable de administrar los controles relacionados con el ambiente físico y las investigaciones relacionadas con incidentes de seguridad.

El área de Auditoría Externa será la responsable de verificar el cumplimiento de las políticas, procedimientos y normas legales aplicables con respecto a la seguridad de la información.

El Concejo Superior Universitario es el responsable de iniciar acciones judiciales, administrativas y/o disciplinarias en caso de violación de la Política y/o las regulaciones de seguridad de la información por parte de los Colaboradores o Terceros.

3.1. Roles y responsabilidades

Para garantizar la gestión de la seguridad de información cada persona vinculada con la UES que utiliza su información, puede estar obligada según las responsabilidades propias de uno o varios de los roles que se definen a continuación:

ROLES	RESPONSABLES
Rol de Usuario de la información	Responsable de conocer y cumplir la Política de Seguridad de la Información, los procedimientos, estándares y legislación aplicable; entender los requerimientos de seguridad y comprometerse con su cumplimiento al acceder y utilizar información en el ejercicio de sus funciones y responsabilidades en la UES.
Rol de Responsable de la Información	Responsable de mantener un nivel adecuado de seguridad de la información que genera o mantiene su área, información que debe clasificar de acuerdo con los criterios de clasificación consignados en esta política.
Rol de Administrador de un sistema de información	Se recomienda que cada sistema de información tenga al menos un administrador autorizado. El administrador es responsable de almacenar información, implementar sistemas de control de acceso (para prevenir divulgación no autorizada), la administración de los usuarios (creación, eliminación, cambio de perfil y depuración de los usuarios) que ingresan al (los) sistema(s) a su cargo y la correcta operación del (los) mismo(s) y ejecutar periódicamente copias de respaldo (para asegurar que la información crítica esté disponible). El administrador también es responsable de desarrollar, aplicar, mantener y revisar las medidas de seguridad definidas por cada Responsable de la información y por el Concejo Superior Universitario.

Rol de Usuario Líder del Sistema de información	Responsable de identificar e implementar mecanismos que controlen el acceso a la información del módulo o aplicación a su cargo teniendo en cuenta las definiciones de seguridad definidas a través de la presente política o por los procedimientos establecidos por el Concejo Superior Universitario para prevenir la divulgación no autorizada. También es responsable de velar porque existan controles que aseguren la disponibilidad de la información crítica.
Rol de Auditor de Sistemas	Verificar el cumplimiento de las políticas y normas del área de informática de la UES. Cabe mencionar que el área de auditoría interna de la UES no cuenta con auditores de sistemas, es por eso que la responsabilidad incluirá la contratación ya sea permanente o temporal de un auditor de sistemas externo dependiendo de la demanda requerida, para la evaluación de la parte de informática y velar por el cumplimiento de políticas y normas.

(Tabla 11 – Roles y Responsabilidades).

4. Definiciones y abreviaturas.

ACCESO: Es el permiso o conjunto de permisos otorgados a los usuarios para ingresar a los recursos informáticos, de acuerdo con las responsabilidades asignadas y las actividades propias del cargo o función.

ACTIVO O RECURSO DE INFORMACIÓN: Es toda la información y los recursos tecnológicos así como los bienes tangibles e intangibles, necesarios o complementarios para el desarrollo de los objetivos del negocio, sin importar su presentación, medio o formato en el que sea creada, exista o sea utilizada.

ADMINISTRADOR DE LA INFORMACIÓN: Persona a cargo de la salvaguarda de la información entregada a su custodia por el Responsable de Información.

AUTENTICACIÓN: Proceso de validación de la identidad del usuario, dispositivo o proceso que intenta acceder al sistema.

AUTORIZACIÓN: Proceso de otorgamiento de privilegios para la ejecución de acciones en el sistema.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

DISPONIBILIDAD: Propiedad que determina que la información sea accesible y utilizable por solicitud de un individuo, área o proceso autorizado o en el momento que se requiera.

ESTÁNDAR: Conjunto de parámetros específicos para cada una de las tecnologías informáticas utilizadas.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Es toda situación relacionada con la condición de un sistema de Información, servicio de red o hardware que identifica o no un riesgo de posible violación de la Política de Seguridad de la Información o falla de los controles implementados.

GESTION DE RIESGO: Proceso mediante el cual se administra y controlan los riesgos.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Un evento o serie de eventos que atentan contra la Confidencialidad, y/o Integridad y/o Disponibilidad de la información y de los recursos tecnológicos que la soportan y que tiene(n) una probabilidad significativa de comprometer las operaciones de la UES y amenazar la seguridad de la información.

INFORMACIÓN CONFIDENCIAL Y PRIVILEGIADA: Es toda la información de la UES cuya divulgación no autorizada compromete los planes, los objetivos estratégicos y/o la reputación de la UES o compromete la responsabilidad de la UES frente a terceros. El número de personas que tienen acceso a este tipo de información es limitado y debe ser controlado estrictamente.

INFORMACIÓN CRÍTICA: Es toda información que se considere indispensable para la realización de un proceso de negocio.

INFORMACIÓN DE USO INTERNO: Información de uso selectivo. Su acceso se basa en la necesidad de conocerla o usarla para cumplir con los procesos de la UES o las funciones de un cargo determinado.

INFORMACIÓN PUBLICA: Información dirigida al público. Su divulgación se hace a través de los canales institucionales establecidos por la UES.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

RIESGO DE TI/INFORMACIÓN: Eventos potenciales relacionados con el uso de la tecnología y/o la información (física o electrónica), los cuales pueden ser explotados por amenazas debido a la presencia de vulnerabilidades, generando un impacto a los procesos de una UES.

SEGURIDAD DE LA INFORMACIÓN: Es el conjunto de medidas de protección que ejerce la UES contra divulgación o modificación no autorizada, hurto o destrucción accidental o intencionada de su información y de la información de terceros que está bajo su cuidado. Estas medidas de protección se basan en el valor relativo de la información y el riesgo en el que se pueda ver comprometida.

TERCEROS: Persona jurídica que provee o presta un servicio a la UES a través de un contrato que es distinto de las personas naturales que están vinculadas con esa persona jurídica.

Fuentes:

- Términos y definiciones ISO/IEC 27001:2005, Sección 3.

5. Contenido de la Política de Seguridad.

5.1. Introducción

La información es un insumo vital para la ejecución de los procesos y la toma de decisiones, además del diseño y definición de los productos y servicios brindados por la UES.

A través del presente documento se establece la Política de Seguridad de la Información, las responsabilidades y los objetivos para la adecuada protección de la Confidencialidad, Integridad, y Disponibilidad de la Información de la UES.

5.2. Principios de la seguridad de la información

Los principios en los cuales se basa la Política de Seguridad de la Información de la UES son:

- La información debe mantener su integridad, independiente de su ubicación (temporal o permanente) y/o medio de transmisión.
- Debe respetarse la privacidad de la información en todo momento.
- La información debe estar disponible cuando sea requerida.
- La confidencialidad de la información debe ser preservada, independiente del medio o formato donde se encuentre.

5.3 Evaluación del riesgo y medidas de control.

La UES realizará periódicamente un análisis de riesgos en términos de seguridad de la información, para determinar o actualizar el nivel de riesgo al que está expuesta y el responsable del mismo.

5.4 Marco de referencia.

La definición de la Política de Seguridad de la Información está alineada con las Normas ISO/IEC 27001:2005, 27002 y 27005, aceptados para la práctica de seguridad de la información.

5.5. Vigencia de la política.

La Política de Seguridad de la Información debe ser revisada anualmente, con el fin de establecer su actualización, vigencia y ajuste acorde a los requerimientos del Concejo Superior Universitario y adecuación ante nuevas necesidades, garantizando su eficacia.

5.5.1. Cumplimiento y violaciones.

El cumplimiento de la política de seguridad es obligatorio, esencial y, en algunos casos, legalmente requerido para tener una adecuada protección ante incidentes de seguridad.

La UES debe programar y ejecutar auditorías a la seguridad de la información que verifiquen el cumplimiento y efectividad de la gestión de la seguridad.

Todas las investigaciones de seguridad realizadas o derivadas de reportes recibidos de violaciones a la política de seguridad, serán conducidas por la Unidad de Gestión de Sistemas de Información y Telecomunicaciones, además serán mantenidas en estricta confidencialidad para preservar la reputación del involucrado hasta que se formalice la acción disciplinaria correspondiente.

5.5.2. Publicación y conocimiento de la Política.

La UES publicará la última versión de la presente política en el portal corporativo de la UES (Sharepoint), asimismo toda actualización se dará a conocer a través de los boletines informativos enviados por medios físicos o electrónicos.

Todos los colaboradores y usuarios que sean vinculados por primera vez con la UES, se les proporcionará una copia de la política de Seguridad y deberán firmar un acta de confirmación de conocimiento y acuerdo con lo especificado en ella, incluyendo las sanciones por incumplimiento.

5.6 Elementos específicos de la política.

5.6.1. Gestión de riesgos de TI / información:

5.6.1.1. "Los riesgos de los activos de información de la UES deben gestionarse de forma que permanezcan en niveles aceptables para la UES."

Los riesgos de TI/Información deben ser identificados, analizados, evaluados, tratados y monitoreados con regularidad, de tal manera que se mantengan bajo control, evitando así pérdidas en la disponibilidad de los servicios, económicas y reputacionales.

Los activos de información de la UES incluyen todos los procesos, equipos, documentos y aplicaciones que almacenan y procesan información:

- Sistemas y procesos administrativos.
- Sistemas y procesos académicos.
- Hardware (computadoras, servidores, etc.)
- Software (aplicaciones).
- Documentación impresa.

Para evaluar los riesgos de los activos de información, se deben utilizar metodologías definidas por el SGSI de la UES.

5.6.2. Gestión de activos de información

5.6.2.1. "Cada activo de información en la UES debe tener asignado un responsable, quien tendrá a cargo la seguridad del mismo."
La información que la UES utilice para el desarrollo de sus objetivos debe estar identificada y tener asignado un responsable, quien la utiliza para el desarrollo de su proceso y es el responsable por su correcto uso.

La Unidad de gestión de sistemas de información y telecomunicaciones deberá tener la documentación completa de todos los activos de información y sus responsables. Sin embargo, cada facultad de la UES deberá encargarse de designar responsables de los activos que maneja.

5.6.2.2. "La información debe clasificarse basada en su valor, sensibilidad, riesgo de pérdida o compromiso, y/o requerimientos legales de retención."

Toda la información, independientemente del medio en el que se encuentre, debe estar clasificada en una de las siguientes tres categorías:

- Confidencial y privilegiada
- Uso interno
- Pública

La Unidad de gestión de sistemas de información y telecomunicaciones será responsable de clasificar la información según los parámetros anteriores.

5.6.3. Uso de los activos o recursos de información del negocio

5.6.3.1 "Los recursos de información son provistos a los usuarios para uso interno".

Los activos de información y recursos informáticos de la UES son exclusivamente para propósitos internos y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido.

La UES se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente y se reserva el derecho de monitorear y supervisar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en esta política.

La UES se encargará de comunicar estas disposiciones a los usuarios durante su período de inducción al ingreso de sus labores. (Cumplimiento del numeral A8 "Seguridad ligada a los recursos humanos" de la declarativa de aplicabilidad).

5.6.3.2. Uso de los servicios de Internet e Intranet.

El Servicio de navegación prestado por la UES es suministrado para el uso de personal autorizado únicamente para propósitos acordes a la rama Universitaria. En todas las ocasiones los intereses y reputación de la UES deben ser protegidos.

Todo mensaje publicado por los Colaboradores de la UES o empresas que prestan servicios al mismo, en un grupo de discusión de Internet (blogs, foros, etc.), red social, boletín electrónico, o en cualquier otro sistema de información público, debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la UES. Únicamente las áreas autorizadas explícitamente por la alta dirección podrán utilizar el nombre de la UES con fines de promoción de la imagen corporativa y aprovechamiento de la tecnología.

5.6.3.3. Uso de los servicios de correo electrónico.

Toda información confidencial incluida en correos electrónicos podrá ser enviada a entidades o redes externas únicamente por el personal debidamente autorizado, siguiendo los lineamientos de clasificación y manejo de la Información.

El envío de comunicaciones con fines corporativos desde cuentas de correos personales y/o públicos no se autoriza.

5.6.3.5. Uso de medios removibles.

La utilización de elementos removibles de almacenamiento (Memorias USB/Flash, CD/DVDs re escribibles, discos duros portátiles, celulares, entre otros) por parte de los usuarios, deberá cumplir los lineamientos estrictamente establecidos por el Concejo Superior Universitario.

5.6.3.6. Uso de documentos físicos.

Está prohibido reutilizar papel de documentos que contengan información confidencial. Los documentos confidenciales que cumplan su tiempo de vida, deberán ser debidamente destruidos, de tal manera que no puedan ser utilizados nuevamente ni legibles por alguien no autorizado.

Los documentos impresos más importantes catalogados como confidenciales son:

- Comprobantes de notas de estudiantes.
- Documentos de evaluaciones (exámenes, parciales, controles de lectura, entre otros).
- Material didáctico para docentes (y en algunos casos estudiantes).

5.6.3.7. Uso de recursos informáticos de seguridad.

Solamente los recursos informáticos de seguridad (tales como: detectores de intrusos, Antivirus, herramientas de escaneo de vulnerabilidades, certificados digitales, etc.) suministrados y/o autorizados por la UES a través de la Unidad de Gestión de Sistemas de Información y Telecomunicaciones se deben utilizar en la protección de los activos de información.

5.6.4. Seguridad en el personal.

5.6.4.1. "la UES proveerá los mecanismos necesarios para asegurar que los colaboradores cumplan con sus responsabilidades en seguridad de la información desde su ingreso hasta su retiro."

Es obligación de los Usuarios / Colaboradores, sin excepción alguna, conocer, respetar, cumplir y hacer cumplir los lineamientos, directrices y procedimientos de Seguridad de la Información de la UES. El cumplimiento de esta política debe ser considerada en la evaluación del desempeño de los empleados.

En el momento que se presente una desvinculación o exista un cambio de roles, todo colaborador o tercero debe hacer entrega de todos los activos de información que le hayan sido asignados y, así mismo, le deben ser retirados los derechos de acceso y privilegios, de acuerdo con los procedimientos definidos en la UES.

5.6.5. Gestión de la seguridad en terceros.

5.6.5.1. "Los terceros que utilizan local o remotamente información de la UES deben cumplir con la Política de Seguridad de la Información."

El uso y acceso local o remoto a la información de la UES por terceros y por empresas relacionadas con la UES, debe ser formalizado por medio de acuerdos que hagan obligatorio el cumplimiento de la presente Política.

En el contrato de servicios se debe incluir un acuerdo de confidencialidad y niveles de servicios en Seguridad de la Información, que detalle sus compromisos en el cuidado de la misma y las penas a que estarían sujetos en caso de incumplirlos.

Adicional debe cumplirse el control A6.2 "Terceros" (Anexo 2 - Declarativa de aplicabilidad del SGSI)

5.6.6. Seguridad física y ambiental

5.6.6.1. "Todas las áreas físicas del negocio deben tener un nivel de seguridad acorde con el valor de la información que se almacena, procesa y/o administra en ellas."

La seguridad física de la UES debe basarse en perímetros y áreas seguras, las cuales serán protegidas por medio de controles circundantes apropiados. Estos deben ser consistentes con el valor de la información que contienen y los derechos mínimos de acceso deben ser otorgados teniendo en cuenta si los sitios de trabajo son permanentes o no.

Los recursos informáticos de la UES deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir su exposición, daño o pérdida.

Todos los colaboradores deben portar de manera permanente y en un sitio visible el carnet de identificación de la UES que facilite su identificación y permita diferenciar a personas que no son colaboradores de la UES.

Lo anterior debe estar en cumplimiento con el control A9 "Seguridad física y ambiental" (Anexo 2 – Declarativa de Aplicabilidad del SGSI).

5.6.7. Gestión de Infraestructura TI y Telecomunicaciones.

5.6.7.1. "Todas las conexiones a redes de la UES deben ser autenticadas para prevenir que la información sea revelada o alterada."

Las conexiones a la red privada de la UES deben realizarse de manera segura para preservar la Confidencialidad, Integridad y Disponibilidad de la información trasmitida sobre la red.

Se requiere la aprobación del responsable de la Información para poder acceder remotamente la información de la UES.

El acceso remoto desde la UES a otras redes externas debe realizarse por razones estrictas de negocio y desde equipos desconectados de las redes internas de la UES o desde equipos autorizados por la Unidad de Gestión de Sistemas de Información y Telecomunicaciones.

5.6.7.2. "Todos los recursos informáticos de la UES deben estar protegidos mediante herramientas y software de seguridad que permitan la protección contra código móvil y malicioso."

Debe existir un programa completo a nivel institucional de protección contra código malicioso en los equipos de la UES.

Los usuarios no deben intentar erradicar el código malicioso de los recursos informáticos por sus

propios medios si el software de protección no puede realizarlo. Si un usuario sospecha que un recurso informático está bajo los efectos de un código malicioso, debe dejar de usar el mismo inmediatamente y debe solicitar asistencia al área de soporte técnico.

5.6.7.3. "Se deben ejecutar respaldos a la información clasificada como confidencial o crítica para la UES."

La UES debe establecer procedimientos para asegurar que toda la información clasificada como confidencial y privilegiada o como información crítica para la UES contenida en su plataforma tecnológica es periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Se deberá definir la periodicidad de la ejecución de los procesos de respaldo de la información crítica de la UES.

Los medios de respaldo de la información de misión crítica de la UES se deben almacenar en localidades alternas y seguras.

La solicitud de restauración de información solo podrá ser realizada por el responsable de la misma o por aquel que él designe.

5.6.7.4. "Los eventos de seguridad de la información de la UES deben ser registrados y revisados permanentemente para asegurar el cumplimiento de los requerimientos de seguridad de la información."

La UES debe establecer los mecanismos adecuados para detectar las actividades que amenacen la Confidencialidad, Integridad y Disponibilidad de la información.

Los recursos informáticos deben incluir registros de auditoría que involucren cualquier evento susceptible de verificación posterior e incluyan la cuenta de usuario que lo generó.

La gestión de incidentes de seguridad de la información debe realizarse acorde al numeral A13 "Gestión de incidentes de seguridad de la información" (Anexo 2 – Declarativa de aplicabilidad del SGSI).

5.6.8. Gestión de accesos a la información.

5.6.8.1. "Todos los usuarios que acceden a la información de la UES deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal."

Cada colaborador o tercero debe tener asignada una única cuenta (Identificador) de usuario para obtener acceso a cualquier recurso informático de la UES, a las plataformas, aplicaciones y sistemas que utilice para el desarrollo de su función o rol dentro de la UES.

En casos excepcionales y previa justificación y aprobación por parte del responsable de la Información se podrán solicitar la creación de cuentas de usuario genéricas, siempre estableciendo a un colaborador de la UES como responsable del uso de la misma.

5.6.9. Incidentes de seguridad de la información.

5.6.9.1. "La UES debe ser alertado en el mismo instante en que existan eventos o situaciones que afecten la Confidencialidad, Integridad y Disponibilidad de la información y/o violaciones a la Política de Seguridad de la Información."

Las situaciones o acciones que violen las políticas, responsabilidades y procedimientos de seguridad de la información deben ser detectadas, registradas e informadas al Concejo Superior Universitario de manera inmediata (alertas). Se debe desarrollar un programa de manejo de incidentes que dé prioridad a dichas alertas y las resuelva conforme a la criticidad de la información para la UES. Dicho programa debe incluir la definición de una Universidad de reacción inmediata, con el objetivo de atender estas y otras situaciones que la UES considere como críticas.

Todos los colaboradores y terceros son responsables por reportar en forma inmediata y mediante los medios destinados para tal fin, cualquier condición anormal o vulnerabilidad que detecte en el uso los recursos informáticos y/o de la información de la UES, así como la violación a la política por parte de

colaboradores o terceros.

La información específica sobre las vulnerabilidades o condiciones anormales de seguridad de la información tiene carácter de confidencial y solo debe darse a conocer a personas autorizadas y que tengan una necesidad demostrada de conocerla.
La UES debe establecer y mantener un procedimiento formal de reporte de incidentes de seguridad de la información que le permita a los usuarios, terceros, filiales y Entidades, informar acerca de éstos cuando se presenten o se tenga sospecha de su ocurrencia.

Todo incidente o alerta de seguridad debe ser tratado de principio a fin mediante un procedimiento de tratamiento de incidentes que garantice el análisis, investigación, documentación, solución completa, seguimiento a los mismos y en algunos casos permita adelantar acciones administrativas/legales correspondientes.

5.6.10. Continuidad del negocio

5.6.10.1. "Todos los procesos críticos del negocio y los recursos de información asociados, deben contar con un plan de continuidad del negocio que permita la normal operación de los mismos ante la ocurrencia de eventos no previstos o desastres naturales."

En caso que los activos de información críticos sufran alguna situación que lleve a la falla en su Disponibilidad, se deben desarrollar, documentar, implementar y probar periódicamente procedimientos que aseguren en primera instancia la preservación del recurso humano además de la continuidad de las operaciones de sus procesos críticos, ante la ocurrencia de eventos no previstos o desastres naturales y que aseguren una recuperación razonable y a tiempo, sin disminuir los niveles de seguridad establecidos.

La UES establecerá medidas de reacción inmediata que permitan detectar y mitigar los efectos de ataques que afecten la Disponibilidad de los servicios (Por ejemplo Denegación de Servicios). Estas medidas estarán fundamentadas en procedimientos y elementos que permitan mantener informado a la UES de la existencia de estas amenazas, detectar los ataques de manera oportuna y ejecutar las acciones consiguientes que restauren la normal prestación de los servicios que se han visto afectados.

La UES deberá garantizar la existencia de un plan de recuperación de desastres, incluido un servicio de contingencia alterno, sobre los recursos informáticos críticos del negocio y la operación, que garantice la continuidad de los procesos de la UES ante eventos catastróficos.

La gestión de continuidad del negocio debe cumplir el control A14 "Gestión de la continuidad del negocio" (Anexo 2 – Declarativa de aplicabilidad del SGSI).

B. Planteamiento de los análisis de riesgo
Se definieron los activos de información de la UES, como se describen a continuación:

ADMINISTRATIVOS			
Nombre	**Descripción**	**Tipo de Sistema**	**Descripción de lo que se debe de garantizar en función de la seguridad.**
Sistema de Colecturías.	Llevar la información de los pagos de certificaciones, exámenes o cualquier trámite extra de la UES	Tradicional	Integridad-Confidencialidad-Disponibilidad
Sistema de control de horas extras	Generación de planillas de horas extras.	Tradicional	Integridad-Confidencialidad
Sistema de Administración de Cuotas de Matrícula y Escolaridad (ACME)	Emisión de talonarios, y registro de los pagos realizados de todas las facultades	Tradicional	Integridad-Confidencialidad-Disponibilidad
Sistema de Gestión de las Adquisiciones y Contrataciones	Gestionar las adquisiciones y contrataciones de bienes, obras y servicios que se realizan por las diferentes entidades de la UES.	Tradicional	Integridad-Confidencialidad

ACADEMICOS-ADMINISTRATIVOS			
Sistema informático para el primer ingreso	Servir de apoyo a los procesos de registro de aspirantes a primer ingreso para cada una de sus fases y a la selección de los mismos.	Tradicional	Integridad-Confidencialidad-Disponibilidad
Certificados de notas (ADACAD)	Gestionar lo referente a la emisión de los certificados de notas de la UES.	Tradicional	Integridad-Confidencialidad-Disponibilidad
Registro Académico (ADACAD)	Gestión de los procesos académicos universitarios de los estudiantes.	Tradicional	Integridad-Confidencialidad-Disponibilidad
Sistema de datos históricos	Registro de movimientos que realiza el estudiante, cuando son procesos centrales o que involucran varias facultades	Tradicional	Integridad-Confidencialidad-Disponibilidad

DOCUMENTOS IMPRESOS			
Registros impresos de comprobantes de notas.	Registros de los comprobantes de notas de cada alumno de la UES.	N/A	Integridad-Disponibilidad
Documentos de evaluaciones.	Documentos de evaluaciones como exámenes parciales, laboratorios, entre otros.	N/A	Integridad-Confidencialidad-Disponibilidad
Material educativo para impartir clases.	Documentos de material didáctico para impartir las clases.	N/A	Integridad-Disponibilidad

HARDWARE			
Servidores de base de datos.	Servidores en donde se almacenan y se procesan la información los cuales sirven de insumo para las aplicaciones.	N/A	Integridad-Confidencialidad-Disponibilidad
Servidores de aplicaciones.	Servidores en donde se encuentran alojadas las aplicaciones.	N/A	Integridad-Confidencialidad-Disponibilidad

(Tabla 12 – Activos de información).

Además, se realizó un análisis a los controles de seguridad establecidos en el Anexo A.0 de la ISO 27001:2005. Los controles se utilizan como una referencia para la implementación de medidas de seguridad y protección de la información; y principalmente para corroborar que estén incorporadas todas las medidas de seguridad.
Se analizaron los objetivos de control para considerar si son necesarios para la UES, dando de esta forma un plan de acción específico para cada control.

Gracias a este ejercicio, se realizó un análisis del riesgo para los activos de la información de la UES, donde se utilizó la información presentada en la ISO 31010 para evaluar cuál era la mejor herramienta a tomar en cuenta para realizar dicho análisis.

Cabe recalcar que el propósito de la valoración del riesgo es suministrar información y el análisis con base en las evidencias que se obtengan como resultados de dichas herramientas, para poder tomar decisiones que sean importantes para la institución, para que se posea un rumbo a la hora de la toma de decisiones sobre la manera de tratar los riesgos tanto internos como particulares.

Con el análisis de riesgo, la UES podrá:
• Comprender el riesgo y el impacto de cada uno de ellos con respecto a los objetivos de la institución.
• Poder brindar información para el personal que toma decisiones.
• Facilitar las opciones del tratamiento de los riesgos identificados.
• Comparación de los riesgos de los sistemas y tecnologías de la institución.

• Cumplir con los requerimientos normativos y reglamentarios.
• Brindar información que ayudará al personal que toma decisiones sobre la aceptación de un riesgo al compararlo con criterios predefinidos.

Al iniciar a implementar el análisis, se realizó una comparación de las técnicas de la valoración del riesgo, y se observó que existen factores que influyeron en la selección del tipo de técnica, como por ejemplo:

• La complejidad del problema y los métodos que se tendrían para validar la información.
• El grado de incertidumbre de la valoración del riesgo.
• La cantidad de recursos de información y el nivel de experticia necesario.
• Y como punto importante, se tomó en cuenta que el método suministre un resultado cualitativo y cuantitativo.

A continuación se especifican, junto con la complejidad, grado de incertidumbre, nivel de experticia y la obtención de un resultado cuantitativo o cualitativo, las técnicas utilizadas para la realización del análisis del riesgo de los activos de la información de la UES:

Herramienta	Complejidad	Grado de incertidumbre	Nivel de experticia	Resultado cuantitativo
Lluvia de ideas	Bajo	Bajo	Bajo	No
Entrevista estructurada y semiestructuradas	Bajo	Bajo	Bajo	No
Análisis de confiabilidad humana.	Medio	Medio	Medio	Si
Análisis en esquema de corbatín	Medio	Alto	Medio	Si
Análisis del impacto en el negocio	Medio	Medio	Medio	No

(Tabla 13 – Técnicas de análisis de riesgos).

Posteriormente se realizó una identificación de los riesgos, según el siguiente detalle:

Sistema / Activo	Descripción del Riesgo	Dueño del Riesgo	Probabilidad Inherente	Impacto Inherente
Sistema de Colecturía	Pérdida de integridad de información de pagos por modificaciones no autorizadas.	Unidad de Tesorería Financiera Institucional	Media	Alto
Sistema de Colecturía	Imposibilidad de realizar trámites por fallas en el sistema.	Unidad de Tesorería Financiera Institucional	Alta	Alto
Sistema de Control de Horas Extra	Cálculo de erróneo de horas extra debido a alteración o pérdida de información.	Unidad de Recursos Humanos	Media	**Bajo**
Sistema de Administración de Cuotas de Matrícula y Escolaridad	Descuadre contable por problemas de comunicación con los sistemas bancarios.	Administración de Cuotas de Matrícula y Escolaridad (ACME)	Media	Alto
Sistema de Administración de Cuotas de Matrícula y Escolaridad	Cobros indebidos a estudiantes por cálculos erróneos debido a modificaciones o mala parametrización del sistema.	Administración de Cuotas de Matrícula y Escolaridad (ACME)	Baja	Medio
Sistema de Gestión de Adquisiciones y Contrataciones	Pérdida de confidencialidad de información debido a una gestión de seguridad de la información por parte del proveedor.	Unidad de Compras de las Facultades y Unidad de Oficinas Centrales	Media	Alto

Sistema Informático para el primer ingreso	Inconsistencias en el proceso de admisión debido a fallas en los flujos o parametrización errónea en el sistema.	Administración Académica	Alta	Medio
Certificados de Notas	Falsificación de información de notas debido a accesos no autorizados.	Secretaría de Asuntos Académicos	Baja	Alto
Certificados de Notas	Errores en los cálculos de notas.	Secretaría de Asuntos Académicos	Baja	Alto
Registro Académico	Inconvenientes para que los estudiantes realicen gestiones académicas debido a inconsistencias en la información.	Decanos	Alta	Medio
Sistemas de Datos Históricos	Pérdida de información debido a fallas en los respaldos almacenados en el sistema histórico.	Secretaría de Asuntos Académicos	Baja	Medio
Todos los sistemas	Pérdida de disponibilidad de sistemas de información debido a: Fallas de comunicación problemas con el aplicativo, Fallas de infraestructura (BDD, Servidor, etc.)	N/A	Alta	Alto
Servidores de base de datos	Perdida de integridad de los datos debido a accesos no autorizados.	Unidad de gestión de sistemas de información.	Alta	Alto
Servidores de aplicación	Falta de disponibilidad debido a falta de balanceo de la carga.	Unidad de gestión de sistemas de información.	Alta	Alto
Registros impresos de comprobantes de notas	Perdida de documentos impresos debido incidentes como inundaciones en las instalaciones.	Secretaría de Asuntos Académicos.	Baja	Bajo
Documentos de evaluaciones	Alteración en las evaluaciones por accesos no autorizados.	Docentes.	Alta	Alto
Material para impartir clases	Perdida del material didáctico debido a la mala ubicación de los mismos.	Docentes.	Media	Medio

(Tabla 14 – Identificación de riesgos).

A continuación se describen todos los riesgos evaluados con sus causas, controles preventivos, controles mitigantes y consecuencias.

Riesgo	Causas	Controles preventivos (causas)	Controles mitigantes	Consecuencias
Pérdida de integridad de información	Accesos no autorizados, Errores humanos, Errores en el aplicativo.	Establecer políticas robustas de control de acceso. Capacitaciones al personal. Pruebas funcionales de los aplicativos.	Procedimiento de verificación de logs de acceso, Cuadre manual de la información, Respaldo periódicos de la información.	Alteración no autorizada de la información. Ingreso de información errónea. Inconsistencia de la información.
Pérdida de integridad de información	Fallas en la red, Fallas en la base de datos, Fallas en el servidor.	Establecer esquemas de alta disponibilidad en la infraestructura que aloja el aplicativo.	Procedimiento para realizar trámites manuales.	Pérdida de capacidad para realizar trámites en el sistema, Demoras en los procesos debido a que el procedimiento manual es más tardado.
Pérdida de integridad de información en horas extra.	Accesos y/o modificaciones no autorizados, Errores humanos en el ingreso	Establecer controles de seguridad robustos, validación de información previa al ingreso en el sistema,	Revisión de logs de acceso al sistema y aplicación de técnicas de informática forense, corrección manual de	Modificación no autorizada de información, inconsistencias en el pago de horas extras, problemas para generar

	de información, errores de procesamiento en el aplicativo.	mejoras en el control de calidad de los aplicativos previo a su pase a producción.	valores erróneos, aplicación de ajustes/parches al sistema para corregir errores.	reportes de horas extra.
Fallas de comunicación con sistemas bancarios.	Fallas en el enlace de comunicación entre UES y los bancos.	Establecer enlaces redundantes y/o contingencias para el intercambio de información.	Envío de información por medios alternativos.	Inconsistencias en la información almacenada por la UES y los bancos.
Pérdida de integridad de información de horas extra.	Accesos y/o modificaciones no autorizados, Errores humanos en el ingreso de información, errores de procesamiento en el aplicativo.	Establecer controles de seguridad robustos, validación de información previa al ingreso en el sistema, mejoras en el control de calidad de los aplicativos previo a su pase a producción.	Revisión de logs de acceso al sistema y aplicación de técnicas de informática forense, corrección manual de valores erróneos, aplicación de ajustes/parches al sistema para corregir errores.	Modificación no autorizada de información, inconsistencias en el pago de horas extras, problemas para generar reportes de horas extra.
Pérdida de confidencialidad de información de la UES.	Mala gestión de la información por parte del proveedor, falta de políticas para el trato a proveedores.	Capacitación a los proveedores, Establecer políticas de seguridad robustas.	Crear controles para la selección de proveedores, Crear políticas de acuerdo de confidencialidad con los proveedores.	Fuga de información, desorden en el manejo de la información
Inconsistencias en el proceso de admisión.	Fallas en el flujo de la aplicación, parametrización errónea en el sistema.	Realizar pruebas controladas de todos los flujos posibles en el ambiente de desarrollo y en el de producción, revisiones previas al paso de producción	Realizar los cambios en la aplicación que estén causando problemas, modificar los parámetros correctamente.	Imposibilidad de continuar con el proceso de admisión, falsos positivos en los procesos de admisión.
		de la parametrización		
Falsificación de información de notas	Accesos no autorizados, falta de medida de seguridad.	Establecer políticas robustas de control de acceso, establecer controles de seguridad.	Procedimiento de revisión de log de acceso, bloquear los puntos débiles en la seguridad de la aplicación.	Alteración no autorizada de las notas, fuga de información.
Errores en los cálculos de notas.	Fallas en el flujo de la aplicación, parametrización errónea en el sistema.	Realizar pruebas controladas de todos los flujos posibles en el ambiente de desarrollo y en el de producción, revisiones previas al paso de producción de la parametrización	Realizar los cambios en la aplicación que estén causando problemas, modificar los parámetros correctamente.	Mal asignación de notas a los estudiantes, falsos positivos de notas.
Inconvenientes para que los estudiantes realicen gestiones académicas	Perdidas de datos, errores en el sistema, problemas en la infraestructura tecnológica, brechas de seguridad	Configuración de políticas de seguridad en Script de red y estándares de programación	Cambios en la configuración de los sistemas.	Pérdida de datos, retrasos en las gestiones de los estudiantes, fraudes electrónicos.
Pérdida de información debido a fallas en los respaldo	Falta de realización de backups de la información.	Definir e implementar procedimientos de respaldo y restauración de la información.	Respaldo de datos y pruebas de restauración, Administrar almacenamiento de datos en línea y fuera de línea.	Información no protegida, Datos sin disponibilidad.
Pérdida de disponibilidad de los sistemas de	Fallas de comunicación, errores en el sistema, fallas en la	Definir niveles operativos de servicio para procesamiento de datos programados	Operar el ambiente en TI en línea con los niveles de servicio acordados y con	Servicio afectado a causa de incidentes en la operación, Tiempo sin servicio por

informaci ón	infraestr uctura.	, protección de datos de salida, y monitoreo de la infraestructu ra.	instrucciones definidas, Manteniendo la infraestructu ra de TI.	incidentes en la operación.
Pérdida de integridad de la informaci ón	Accesos no autorizad os, actualiza ciones no autorizad as.	Establecer políticas de control de acceso, establecer políticas a seguir para la modificación de la data.	Verificar los accesos a las áreas en donde se encuentra la información, revisión de logs para verificar las actualizacion es.	Alteración de la información
Falta de disponibil idad de las aplicacion es	Mala administr ación de balanceo de carga, mala administr ación en ubicació n de aplicacio nes.	Adquirir mejor software que se encargue del balanceo de carga, establecer control de los tipos de aplicaciones y medir que tan robustas son.	Balancear la carga de acceso a las aplicaciones, Administrar mejor las aplicaciones.	Falta de disponibilida d de las aplicaciones.
Pérdida de document os impresos.	Falta de manteni miento en instalaci ones, mala ubicació n de la documen tación.	Realizar mantenimien to constante en las instalaciones , administrar la documentaci ón.	Realizar mantenimien tos en las instalaciones , buscar una mejor ubicación de la documentaci ón.	Pérdida de documentaci ón.
Alteració n de evaluacio nes.	Falta de control de acceso físico a las instalaci ones, falta de controles para la administr ación de las evaluaci ones.	Establecer controles de acceso, establecer procesos para la administraci ón de evaluaciones .	Verificar los accesos a las áreas en donde se encuentra la información.	Alteración de las evaluaciones o robo de las mismas.
Pérdida de material didáctico.	Mala ubicació n de la documen tación, fala de control de la	Mejor ubicación de la documentaci ón, establecer controles para el	Buscar una mejor ubicación de la documentaci ón, administrar	Pérdida de material didáctico.
	informac ión almacena da.	almacenamie nto de la información.	mejor la información.	

(Tabla 15 – Evaluación de riesgos).

Se evaluó cada uno de los activos con el análisis del corbatín, como se mostró en la tabla anterior, sin embargo, se muestran los esquemas considerados como los más críticos. En la investigación se realizó el análisis del corbatín para todos los activos encontrados.

Activo: Sistema de Colecturía.
Descripción del Riesgo: Pérdida de integridad de información de pagos por modificaciones no autorizadas.

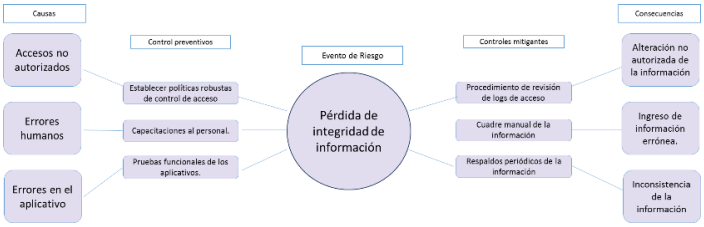

Fig. 1. Análisis Corbatín Riesgo 1 Sistema de colecturía.

Activo: Sistema de Colecturía.
Descripción del Riesgo: Imposibilidad de realizar trámites por fallas en el sistema.

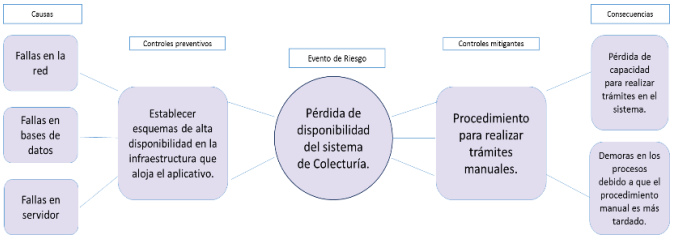

Fig. 2. Análisis Corbatín Riesgo 2 Sistema de colecturía.

Activo: Sistema de Administración de Cuotas de Matrícula y Escolaridad.
Descripción del Riesgo: Descuadre contable por problemas de comunicación con los sistemas bancarios.

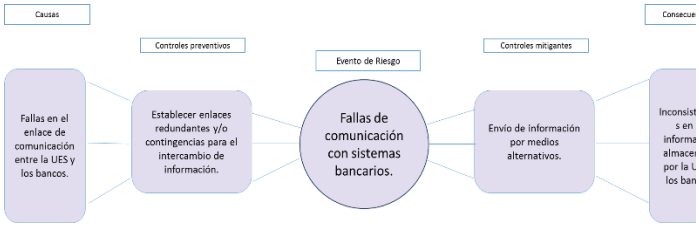

Fig. 3. Análisis Corbatín Riesgo 1Sistema de admin. cuotas.

Activo: Sistema de Administración de Cuotas de Matrícula y Escolaridad.
Descripción del Riesgo: Cobros indebidos a estudiantes por cálculos erróneos debido a modificaciones o mala parametrización del sistema.

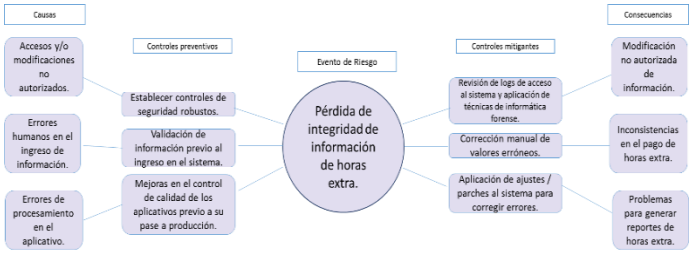

Fig. 4. Análisis Corbatín Riesgo 2 Sistema de admin. cuotas.

Activo: Sistema de Gestión de Adquisiciones y Contrataciones.
Descripción del Riesgo: Pérdida de confidencialidad de información de la UES debido a una mala gestión de seguridad de la información por parte del proveedor/tercero.

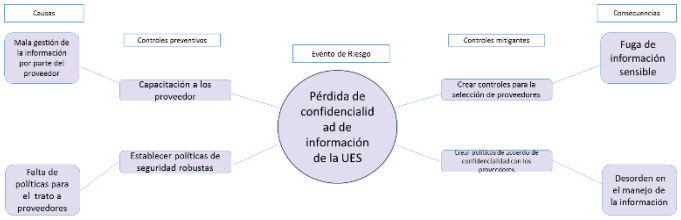

Fig. 5. Análisis Corbatín Riesgo 1 Sistema de Gestión de Adquisiciones y Contrataciones.

Activo: Sistema Informático para el primer ingreso.
Descripción del Riesgo: Inconsistencias en el proceso de admisión debido a fallas en los flujos o parametrización errónea en el sistema.

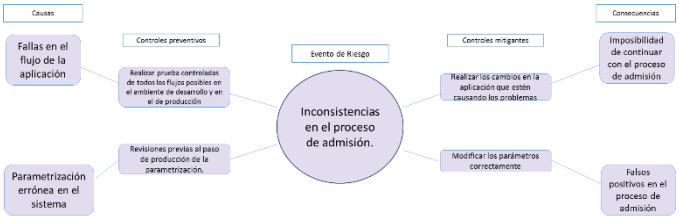

Fig. 6. Análisis Corbatín Riesgo 1 Sistema informático primer ingreso.

Activo: Todos los sistemas.
Descripción del Riesgo: Pérdida de disponibilidad de los sistemas de información debido a: Fallas de comunicación, Problemas con el aplicativo, Fallas de infraestructura (BDD, Servidor, etc.).

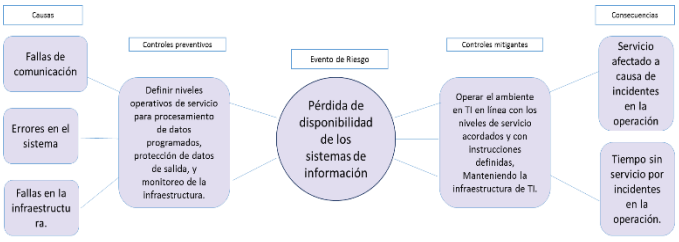

Fig. 7. Análisis Corbatín Riesgo 1 Todos los sistemas.

Activo: Servidores de Base de Datos
Descripción del Riesgo: Perdida de integridad de los datos debido a accesos no autorizados.

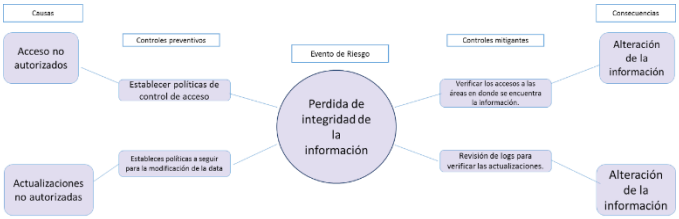

Fig. 7. Análisis Corbatín Riesgo 1 Todos los sistemas.

Con base en lo anterior se recomienda:

- Contemplar los procedimientos que sean convenientes y apropiados para la planificación e implementación de controles de seguridad, basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

- Con la propuesta sobre la implementación de un SGSI, la UES conocerá los riesgos que se han identificado y los debe minimizar y controlar, utilizando la metodología presentada y

especialmente que sea conocida por todos los colaboradores de la UES, la cual pueda ser monitoreada y mejorada de forma frecuente.

C. Cronogramas de los proyectos para la mitigación de riesgos.

A continuación se describe una propuesta de proyectos para la implementación del SGSI en la UES.

PROYECTO 1

MESA DE TRABAJO CON EL CONSEJO SUPERIOR UNIVERSITARIO	
Personal	Autoridad del Consejo Superior Universitario.
	Encargado de Seguridad de la Información
	Encargado de la Planificación
	Encargado de los procesos de la UES
	Jefe de Operaciones
Planificación de actividades	- Crear y establecer una política de la seguridad de la información. - Cumplir con los objetivos y alcances propuestos del SGSI. - Evaluar los roles y responsabilidades de la seguridad de la información contenidos en la política. - Asignar recursos suficientes para la implementación del SGSI. - Realizar revisiones del SGSI. - Asegurar la implementación de Auditorías Internas.

(Tabla 16 – Proyecto 1 Mitigación de riesgos).

PROYECTO 2

ASIGNACIÓN DE LOS RECURSOS PARA LA IMPLEMENTACIÓN DEL SGSI	
Personal	Autoridad del Consejo Superior Universitario.
	Encargado de Seguridad de la Información.
	Encargado de la Planificación.
	Encargado de los procesos de la UES.
	Encargado del centro de cómputo.
	Jefe de Operaciones
Planificación de actividades	- Establecer, implementar, monitorear y revisar el SGSI. - Garantizar que los procedimientos implementados de la seguridad cumplan los requerimientos específicos de la UES. - Aplicar controles que hayan sido implementados para mantener la óptima seguridad de la información. - Verificar mejoras sobre la implementación y el procedimiento del SGSI. - Mejorar eficacia del SGSI.

(Tabla 17 – Proyecto 2 Mitigación de riesgos)

PROYECTO 3

FORMACIÓN Y CONCIENTIZACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN.	
Personal	Autoridad del Consejo Superior Universitario.
	Encargado de Seguridad de la Información.
	Encargado de la Planificación.
	Encargado de los procesos de la UES.
Planificación de actividades	- Determinar las competencias necesarias para el personal que realicen tareas de la seguridad de la información. - Realizar capacitaciones a personal que esté a cargo de la seguridad de la información. - Mantener registro de las capacitaciones impartidas, habilidades, experiencias de cada uno del personal.

(Tabla 18 – Proyecto 3 Mitigación de riesgos)

PROYECTO 4

REVISIÓN DEL SGSI	
Personal	Encargado de Seguridad de la Información.
	Encargado de la Planificación.
	Encargado de los procesos de la UES.
Planificación de actividades	- Verificar los resultados de auditorías del SGSI. - Información sobre revisiones preventivas y correctivas. - Resultados de mediciones de eficacia. - Vulnerabilidades o amenazas que no han sido tratados oportunamente. - Recomendaciones de mejora.

(Tabla 19 – Proyecto 4 Mitigación de riesgos)

PROYECTO 5

CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN	
Personal	Encargado de Seguridad de la Información
	Encargado de la Planificación
	Encargado de los procesos de la UES
	Encargado del centro de computo
	Jefe de Operaciones
Planificación de actividades	- Identificación de activos de información. - Análisis de riesgos de activos identificados. - Priorización de activos basados en la criticidad de los riesgos asociados. - Planificación de mitigación de riesgos. - Ejecución de planes de mitigación por las áreas involucradas/responsables.

(Tabla 20 – Proyecto 5 Mitigación de riesgos)

PROYECTO 6

CONTROL DE ACCESOS	
Personal	Encargado de Seguridad de la Información
	Encargado de los procesos de la UES
	Encargado del centro de computo
	Jefe de Operaciones
Planificación de actividades	- Identificación de los requerimientos de la seguridad de cada una de las aplicaciones utilizadas. - Identificar normas y leyes nacionales, con respecto a la protección del acceso a los datos. - Definir perfiles de acceso del personal, dependiendo la categoría del puesto de trabajo. - Identificar el control de acceso del personal evitando la existencia de múltiples perfiles. - Entregar al personal un detalle de los derechos de acceso según su perfil. - Almacenar las contraseñas en sistemas informáticos protegidos.

(Tabla 21 – Proyecto 6 Mitigación de riesgos)

PROYECTO 7

VALIDACIÓN DE TRANSACCIONES DE BASES DE DATOS	
Personal	Encargado de los procesos de la UES
	Encargado del centro de computo
	Jefe de Operaciones
Planificación de actividades	- Adquirir servidores de base de datos suficientemente robustos para que tenga la capacidad de centralizar la información de todas las facultades. - Realizar mantenimientos a los servidores periódicamente. - Creación de procedimientos de revisión constantemente para validar que se estén creando y utilizando los índices adecuadamente. - Crear procedimientos de limpieza y realización de backups a las tablas de las bases de datos para un mejor rendimiento.

(Tabla 22 – Proyecto 7 Mitigación de riesgos)

Para llevar a cabo los proyectos propuestos, se ha recomendado realizar el siguiente cronograma:

Concepto	Recursos	Inicia	Finaliza
Proyecto 1	Lluvia de ideas, conocimiento del frente de la UES.	01-ene-16	31-mar-16
Proyecto 2	Mapa de procesos, controles y mejoras.	01-abr-16	30-jun-16
Proyecto 3	Carteleras informativas, correos, charlas, etc.	01-feb-16	15-dic-16
Proyecto 4	Auditorías mediciones de eficacia, vulnerabilidad y amenazas.	01-jul-16	31-dic-16
Proyecto 5	Activos, Planes de mitigación, análisis de riesgos.	01-ene-16	29-feb-16
Proyecto 6	Normas, leyes, perfiles de acceso.	01-jul-16	30-sep-16
Proyecto 7	Servidores, procedimientos definidos, backups.	01-oct-16	31-dic-16

(Tabla 23 – Proyecto 8 Mitigación de riesgos)

VI. BENEFICIOS DE LA IMPLEMENTACIÓN DE UN SGSI

Aplica una arquitectura de gestión de la seguridad que identifica y evalúa los riesgos que afectan al negocio, con el objetivo de implantar contramedidas,

procesos y procedimientos para su apropiado control, tratamiento y mejora continua.

Ayuda a las empresas a gestionar de una forma eficaz la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de contramedidas, por implantar controles desproporcionados y de un costo más elevado del necesario, por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno, por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, etc.

VII. CONCLUSIONES

- La gestión de la seguridad de la información debe ser transversal a todas las áreas, facultades y/o departamentos de la UES; además de reconocer que no es un tema estrictamente de TI, sino también engloba áreas administrativas y estudiantes.

- La UES, como organización que maneja información confidencial de sus estudiantes y colaboradores, necesita implementar un SGSI eficiente y adaptable, sin interrumpir sus procesos de negocio.

- Para que la UES pueda implementar adecuadamente los proyectos propuestos, es necesario que se asigne personal dedicado a cada tarea, además de concientizar a todos los involucrados sobre la importancia de los mismos.

VIII. REFERENCIAS

[1] Leonardo Castillo, Henry Flores, Oscar Rodríguez; Sistema para la implementación, mantenimiento y monitoreo de un SGSI para la Universidad Don Bosco.

[2] ISO/IEC 27001:2005 Requerimientos para implementación de un Sistema de Gestión de Seguridad de la Información.

[3] ISO 31000:2009 Gestión de riesgos, principios y Directrices.

[4] ISO/IEC 31010 Gestión de riesgos, evaluación del riesgo y evaluación de técnicas del riesgo.