UNIVERSIDAD DON BOSCO (UDB)

FACULTAD DE INGENIERÍA

ESCUELA DE COMPUTACIÓN

Normalizaciones y Estándares (C2 - 2014)

Perfil de Tarea Exaula No. 3.

MODALIDAD DE LA ASIGNACIÓN

Trabajo cooperativo: El trabajo se realizará en grupos únicamente con un mínimo de **3 integrantes** y máximo de **4 integrantes.**
La asignación corresponde a una investigación en la cual se pretende fortalecer sus conocimientos en el tema asignado.
Debe ser redactada de manera clara y precisa, en la cual necesariamente debe citar libros de texto, no solamente material de Internet.
La investigación deberá entregarse en un archivo en formato PDF a través del aula virtual en la plataforma My Pizarron.

NO SE RECIBIRÁN TRABAJOS QUE NO CUMPLAN ESTOS REQUISITOS.

OBJETIVOS

- Conocer la normativa ISO 27000 y sus áreas de aplicación.
- Identificar los distintos aspectos relevantes de la normativa, sus alcances, limitaciones y lineamientos.

PONDERACIÓN

El presente reporte tiene una ponderación del **25 %** de la nota del **Segundo Período**, considerando una escala de calificación de 0 a 10.

CONTENIDO DE LA INVESTIGACIÓN BIBLIOGRÁFICA

El documento digital deberá contener la siguiente estructura:

1. Carátula con el nombre completo y carnet de los integrantes
2. Índice
3. Introducción
4. Desarrollo de la Investigación
5. Conclusiones
6. Fuentes de Consulta

DESCRIPCIÓN Y LINEAMIENTOS DE LA TAREA

Debe realizarse una investigación bibliográfica acerca de los siguientes temas:
En la unidad III de la asignatura se ha abordado uno de los estándares de calidad aplicados a la gestión de seguridad de la información (SGSI), el estándar ISO 17799 (actualmente ISO/IEC 27002).
Esta norma es parte de una gran familia de normas, la familia de normas 27000.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares que proporcionan un marco para la gestión de la seguridad.
Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.
Esta serie de normas o familia de Estándares Internacionales para Sistemas de Gestión de la Seguridad de la Información (SGSI) (ISMS por sus siglas en inglés), incluye requerimientos de sistemas de gestión de seguridad de la información, gestión del riesgo, métricas y medidas, guías de implantación, vocabulario y mejora continua.

Debido a ello, es de suma importancia, conocer sobre estas normativas que sirven de apoyo a un profesional de TI, para la implementación de un SGSI.
Por lo tanto, la presente investigación se centrará en la familia de normas ISO 27000, la cual está compuesta por las siguientes normas:

- **ISO/IEC 27000:** define el vocabulario estándar empleado en la familia 27000 *(definición de términos y conceptos).*

- **ISO/IEC 27001:** especifica los requisitos a cumplir para implantar un SGSI certificable conforme a las normas 27000.

- **ISO/IEC 27002:** código de *buenas prácticas* para la gestión de la seguridad. **(Estudiada en la unidad III, no será parte de la investigación).**

- **ISO/IEC 27003**: Guía de implementación de SGSI e información acerca del uso del modelo PDCA (Plan-Do-Check-Act) y de los requerimientos de sus diferentes fases.

- **ISO/IEC 27004:** especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.

- **ISO/IEC 27005:** gestión de riesgos de seguridad de la información (recomendaciones, métodos y técnicas para evaluación de riesgos de seguridad).

- **ISO/IEC 27006:** requisitos a cumplir por las organizaciones encargadas de emitir certificaciones ISO/IEC 27001.

- **ISO/IEC 27007:** guía de actuación para auditar los SGSI conforme a las normas 27000.

- **ISO/IEC 27008:** Consiste en una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

- **ISO/IEC 27010:** Es una norma en 2 partes, que consiste en una guía para la gestión de la seguridad de la información en comunicaciones inter-sectoriales.

- **ISO/IEC 27011:** Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-T X.1051.

- **ISO/IEC 27012:** Consiste en un conjunto de requisitos (complementarios a ISO/IEC 27001) y directrices (complementarias a ISO/IEC 27002) de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración.

- **ISO/IEC 27013:** Consiste en una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

- **ISO/IEC 27014:** Consiste en una guía de gobierno corporativo de la seguridad de la información.

- **ISO/IEC 27015:** Consiste en una guía de SGSI para organizaciones del sector financiero y de seguros.

- **ISO/IEC 27031:** guía de continuidad de negocio en lo relativo a tecnologías de la información y comunicaciones (en desarrollo).

- **ISO/IEC 27032:** guía relativa a la ciberseguridad (en desarrollo).

- **ISO/IEC 27033:** Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales, 27033-2, directrices de diseño e implementación de seguridad en redes; 27033-3, escenarios de redes de referencia; 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad; 27033-5, aseguramiento de comunicaciones mediante VPNs; 27033-6, convergencia IP; 27033-7, redes inalámbricas.

- **ISO/IEC 27034:** Consiste en una guía de seguridad en aplicaciones informáticas.

- **ISO/IEC 27035:** Consiste en una guía de gestión de incidentes de seguridad de la información.

- **ISO/IEC 27036:** Consiste en una guía de seguridad de outsourcing (externalización de servicios).

- **ISO/IEC 27037:** Consiste en una guía de identificación, recopilación y preservación de evidencias digitales.

Para cada norma se considerarán los siguientes aspectos:

I. Descripción detallada de la norma.
II. Objeto y campo de aplicación.
III. Alcances y Limitantes.
IV. Beneficios de utilizar la norma.
V. Importancia de la norma.
VI. Aspectos importantes que trata la norma (lo que se norma y cómo se norma).
VII. Cómo se implementa la norma.

Deberá elaborarse un documento digital conteniendo la investigación realizada, este documento deberá ser de tipo PDF.
Deberán incluir las normas utilizadas en la investigación (en formato digital) o en su defecto las referencias (URL's) donde las consultaron.
El documento conteniendo el resultado de la investigación y las normas consultadas deberán incluirse en un archivo de tipo comprimido (ZIP, RAR), y será este archivo comprimido, el que deberá ser enviado a través del aula virtual en la plataforma My Pizarron, en la fecha indicada en este documento.

CRITERIOS A EVALUAR

- Entrega Puntual del trabajo	5 %
- Creatividad en la forma de presentar la información	5 %
- Presentación digital del reporte	
Carátula, Índice, Introducción	10 %
Contenido del reporte	40 %
Ortografía y Redacción	10 %
Conclusiones	15 %
Fuentes de Consulta (documentos normativos consultados)	15 %

INFORMACIÓN DE INTERÉS GENERAL

- Los trabajos extemporáneos quedan a discrecionalidad del Profesor recibirlos; en todo caso sujetos a la correspondiente justificación y nueva ponderación.
- El plagio es visto como una falta grave dentro del proceso de formación académica de los estudiantes, por cuanto este tipo de acciones será penalizada con la anulación del trabajo, perdiendo el estudiante su derecho a apelación y/o reevaluación de dicha actividad.

FECHA Y HORA DE ENTREGA LIMITE

26 de Septiembre de 2014 a las 11:55 PM (23:55 horas, HORA DEL SERVIDOR) a través de la plataforma My Pizarron

NO SE RECIBIRÁN TRABAJOS POR CORREO ELECTRÓNICO.