DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA

ISO/IEC 27001:2013

TRABAJO DE GRADO

PARTICIPANTES

ARLENYS CAROLINA NIEVES

1422010372

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Ciudad, Fecha

TABLA DE CONTENIDO

INTRODUCCIÓN

La información y los procesos que se desarrollan para las actividades de las empresas y/o Entidades asumen muchos riesgos, por ello se deberían emplear medidas de control sobre la seguridad de la información y activos informáticos que involucre a todo el personal, desde la alta dirección hasta los operarios de los sistemas.

La información hoy por hoy está disponible para los usuarios internos como externos, desde dispositivos de computo (Tablet, Laptop, etc.), aplicaciones web, aplicaciones internas, conexiones de red (Intranet), por lo tanto, la seguridad es un elemento fundamental, al cual se debe dar prioridad porque con ello se garantizan confidencialidad, integridad y disponibilidad de los sistemas de información e informáticos. Las amenazas y las vulnerabilidades que se presentan en los sistemas y activos de información, involucran desde el desarrollo de las actividades de los empleados hasta los mecanismos de acceso a los mismos.

Lo anterior es conocido como Sistema de Gestión de la Seguridad de la Información y está basado en estándares, modelos y normas internacionales que a través de una serie de mejores prácticas aseguran una adecuada gestión de la seguridad de la información.

Una de las normas más reconocidas es la ISO/IEC 27001:2013 que establece las guías, procedimientos y procesos para gestionarla apropiadamente mediante un proceso de mejoramiento continuo.

El presente proyecto busca analizar e implementar un sistema de gestión de seguridad de la información usando la norma ISO 27001 :2013 y la metodología MAGERIT para la gestión del riesgo en los activos de información del Centro de Educación Técnica y Tecnológica del departamento del Cesar.

AGRADECIMIENTOS

A Dios, a mi madre María Francisca Nieves y demás familiares, quienes siempre han confiado en mí y me han dado su apoyo incondicional.

1. Resumen Ejecutivo

El contenido de este trabajo es una guía, que permitirá evaluar la integridad, confidencialidad y disponibilidad de los activos (Hardware - Software) de información a las oficinas de Ingreso de Centros de Educación Técnica y Tecnológica del Cesar.

Para el desarrollo de lo anterior, se dividió en tres fases: Planeación, incluyó un análisis de situación y descripción de los procesos, en la fase de Preparación incluyó GAP análisis, activos de información (análisis y evaluación de riesgos), y la última fase Capacitación y sensibilización, en donde se involucra la concientización de seguridad de sistemas y activos de información.

El alcance del trabajo abarcará el diseño de un SGSI, que cubrirá las necesidades para mitigar los riesgos a los que está expuesta la Entidad. Además, servirá como una guía ajustable a cualquier Centro de Educación Técnica y Tecnológica.

El trabajo solo consistirá en el diseño de SGSI de la oficina de Ingreso del Centro de Educación Técnica y Tecnológica del departamento del Cesar, todo lo anterior, se desarrolla dentro del marco conceptual y metodológico de un sistema de gestión de seguridad de información bajo la norma ISO 27001:2013.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Diseño de un sistema de gestión de seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013

1.2.2. OBJETIVOS ESPECÍFICOS

- Realizar un GAP análisis basados en la norma ISO/IEC 27001:2013.
- Definir una metodología para la identificación y clasificación de los activos de información.
- Establecer una valoración y tratamiento de riesgos de Seguridad de la Información a los Activos de información.
- Realizar un cronograma de capacitaciones en seguridad de la información.

1.3 RESULTADOS OBTENIDOS.

- Análisis de GAP.

  A través de la aplicación de dos (2) test, se verificó la situación real de la oficina de Ingreso del Centro de Educación Técnica y Tecnológica del departamento del Cesar, lo anterior permitió identificar:

  a) Estado actual
  b) Expectativa a futuro
  c) Brecha
  d) Mejora

- Metodología de Riesgos de Seguridad de la Información de los activos de información.

  Se procedió a realizar las siguientes actividades:

  a) Gestión y clasificación de los activos de información
  b) Identificación y valoración de las amenazas
  c) Análisis del riesgo

- Plan de capacitación de Seguridad de la Información.

  Se procederá a realizar las siguientes actividades:

  a) Actividades a desarrollar en el plan de concienciación

- Administración y buen uso de contraseñas y accesos a los sistemas de información.
- Seguridad de los puestos de trabajo.
- Uso responsable de activos de información (Hardware - Software).
- Cronograma de actividades.
- Análisis de riesgos de los activos de información.

b) Seguimiento a la capacitación.

1.4 ALCEN Y LIMITACIONES

El desarrollo del trabajo abarca el diseño de un sistema de Gestión de Seguridad de la información en la oficina de Ingreso del Centro de Educación Técnica y Tecnológica del departamento del Cesar, además de la valoración y clasificación de los activos de información.

Todo lo anterior, soportado con la norma ISO/IEC 27001:2013, y metodología de análisis de riesgo MAGERIT.

Este trabajo no abarca implementación, mantenimiento y revisión del Sistema de Gestión de Seguridad de la Información.

2. JUSTIFICACION

La seguridad de la información surge como una medida de asegurar que la información tenga los niveles adecuados de protección en cuanto a Confidencialidad, Integridad y Disponibilidad.

La creciente cantidad de amenazas que sufren las organizaciones al interior y exterior de los sistemas de información, hace que crezca la necesidad de gestionar de manera eficiente los riesgos e involucrar al personal y capacitarlo para hacerle frente a dichas amenazas, minimizando el impacto para la entidad, según DELOITTE[1] en la encuesta 2016 sobre Tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica, en su página 10, se describe las Principales Tendencias Identificadas, en la cual se identifica en cuarto lugar "la capacitación y concientización es la iniciativa de seguridad que mayor cantidad de organizaciones ejecutaran durante 2016". Además, la revista DINERO[2], hace referencia que el 2015 fue un año de "altas y bajas" para la seguridad informática," Colombia es considerada una de las naciones más atractivas para los delincuentes informáticos en América Latina, muestra de ello es que el 25% de los ciberataques registrados en el 2015 se originaron en esta parte del mundo".

Un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013, proveerá las condiciones necesarias para que la seguridad de la información apoye y extienda los objetivos estratégicos de la Entidad, para garantizar la debida gestión administrativa y operativa.

Un propicio Modelo de Seguridad de la Información en la Entidad le proporcionará las herramientas y elementos necesarios para alcanzar de manera efectiva los siguientes objetivos de seguridad:

[1]https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%C3%A9rica%20-%20Resultados%20Generales%20vf%20(Per%C3%BA).pdf

[2] http://www.dinero.com/pais/articulo/informe-certicamara-sobre-seguridad-informatica-colombia-para-2016/217635

- Asegurar la integridad y continuidad de los servicios (Internet, Correo electrónico, carpetas en red, etc.), equipos y sistemas de información, así como el acceso a los mismo.

- Uso adecuado en cuanto a la confidencialidad de claves y/o passwords de los sistemas de información.

- Generar sentido de pertenencia y apropiación en temas de seguridad en los funcionarios de la entidad, para logrando con ello la participación activa en controles y medidas orientadas a salvaguardar la seguridad de la información de la Entidad.

El desarrollo del presente ante-proyecto busca satisfacer la necesidad de seguridad de la información de sus activos y el recurso humano, garantizando la confidencialidad, disponibilidad e integridad de los datos.

3. MARCO TEÓRICO Y REFERENTES

3.1 MARCO TEÓRICO

Para el desarrollo de un sistema de gestión de seguridad de la información se utilizan conceptos referentes a la seguridad que aplican a cualquier tipo de entidad, públicas y/o privadas.

Sistema de Gestión de la Seguridad de la Información[3]- SGSI: es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad**: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad**: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

[3] http://www.iso27000.es/download/doc_sgsi_all.pdf

- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

ISO 27001[4]: es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ANÁLISIS DE RIESGO: es el proceso cuantitativo o cualitativo que permite evaluar los riesgos. El primer paso del análisis es identificar los activos a proteger o evaluar. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente. La función de la evaluación consiste en ayudar a alcanzar un nivel razonable de consenso en torno a los objetivos en cuestión, y asegurar un nivel mínimo que permita desarrollar indicadores operacionales a partir de los cuales medir y evaluar. Los resultados obtenidos del análisis, van a permitir aplicar alguno de los métodos para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos. Dentro del tema de análisis de riesgo se ven reflejados cinco elementos

[4] https://advisera.com/27001academy/es/que-es-iso-27001/

muy importantes dentro del concepto estos son los siguientes: probabilidad, amenazas, vulnerabilidades, activos e impactos.

MAGERIT: es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.

- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

CICLO DE MEJORA CONTINÚA EN LA NORMA ISO/IEC 27001:2013

Plan: Consiste en planificar acciones para hacer frente a los riesgos e identificar las oportunidades, para posteriormente evaluarlas y gestionarlas.

- Definir las políticas de seguridad de la información
- Establecer el alcance del SGSI
- Realizar el análisis de riesgo
- Seleccionar los controles de seguridad
- Definir competencias
- Establecer el mapa de riesgos
- Definir autoridades y responsabilidades

Hacer: Indica que la organización debe de disponer los recursos necesarios para establecer, implementar y mantener el SGSI, además de dar a conocer las políticas de seguridad de la información del SGSI.

- Poner en marcha el Plan de gestión de riesgos establecido
- Se implanta el SGSI
- Se establecen los controles de seguridad

Check – Controlar

- Revisar internamente el SGSI
- Realizar auditorias
- Se revisan los indicadores y métricas del SGSI

Actuar

- Realizan las acciones correctivas
- Realizan las acciones preventivas

3.2 MARCO CONCEPTUAL

ACTIVOS: Los activos a reconocer son aquellos relacionados con sistemas de información. Ejemplos típicos son los datos, el hardware, el software, servicios, documentos, edificios y recursos humanos.

IMPACTOS: las consecuencias de la ocurrencia de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo.

AMENAZAS: las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

GESTIÓN DEL RIESGO: Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

VULNERABILIDAD: Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

4. METODOLOGÍA

4.1 Tipo de investigación: Se desarrolló una metodología cuantitativa y cualitativa tomando como referencia los anexos de la ISO/IEC 27001:2013.

4.2 Línea de investigación. Como referencia para el desarrollo del trabajo se utilizó la norma ISO/IEC 27001:2013, abordando los temas de tecnología de la información, gestión de la seguridad y seguridad de la información.

4.3 Instrumentos de recolección de información. Para el desarrollo del trabajo se utilizó el cuestionario, entrevistas y la observación de los funcionarios en el desarrollo de sus actividades. También fue utilizado diferentes fuentes de información, tales como tesis, textos, revistas, etc., en medios electrónicos.

4.4 Fases metodológicas. Para la realización de los entregables se desarrolló dos (2) test, en base a la norma ISO/IEC 27001:2013, los cuales se utilizaron Anexos y capítulos.

- Los controles del anexo A, agrupados y numerados de la siguiente forma:
  A.5 Política de seguridad
  A.6 Organización de la información de seguridad
  A.7 Administración de recursos
  A.8 Seguridad de los recursos humanos
  A.9 Seguridad física y del entorno
  A.10 Administración de las comunicaciones y operaciones
  A.11 Control de accesos
  A.12 Adquisición de sistemas de información, desarrollo y mantenimiento
  A.13 Administración de los incidentes de seguridad
  A.14 Administración de la continuidad de negocio
  A.15 Cumplimiento.

Capítulos:

Número 4, Contexto de la Organización

Número 5, Liderazgo

Número 6, Planificación

Número 7, Soporte

Número 8, Operación

Número 9, Evaluación del Desempeño

Número 10, Mejora

Análisis y gestión de riesgo:

a) Identificación de los activos de información**.**

b) Amenazas – vulnerabilidad – riesgo

c) Valoración de riesgo

d) Plan de tratamiento

e) Matriz de riego.

Capacitación seguridad de la información.

- Sensibilizar sobre las responsabilidades de los activos de la información a funcionarios, contratistas y personal de apoyo.
- Concientizar a funcionarios, contratistas y personal de apoyo de la entidad de la importancia de la seguridad de la información en cuanto a la confidencialidad, integridad y disponibilidad.
- Sensibilización de los controles de seguridad y la relación que tienen con los activos (Hardware - Software) de la información que manejan

5. RESULTADOS Y DISCUSIÓN

La oficina de Ingreso del Centro de Educación Técnica y Tecnológica del departamento del Cesar

Objetivo

Establecer las actividades para garantizar los medios y recursos para el registro e inscripción de los aspirantes y/o empresas en los programas de formación profesional, para que a través de la utilización de instrumentos de evaluación se seleccionen aquellos aspirantes que cumplan con las competencias mínimas requeridas y formalizar su ingreso mediante la matricula.

Descripción del funcionamiento del área de Ingreso.

Se desarrollan en tres actividades principales:

1. Registro e Inscripción: Es el registro de datos básicos en el aplicativo de gestión académica de la Entidad y posterior inscribirse a un programa de formación.

Se desarrollan en tres actividades principales:

1. **Registro e Inscripción:** Es el registro de datos básicos en el aplicativo de gestión académica y posterior inscribirse a un programa de formación.

Entradas	Actividades	Salidas
Resolución de Calendario Académico y de Labores y	Registro de aspirante a la formación.	Registro e inscripción en el aplicativo de gestión académica.
	Inscripción de aspirante a la formación.	

Cronograma para cada convocatoria.	Generar un reporte de inscritos a la formación.	Reporte de Inscritos

2. **Selección:** Es la actividad mediante la cual se verifican conocimientos, aptitudes y actitudes de los aspirantes a la formación profesional de acuerdo con lo establecido en el perfil de ingreso esperado para cada programa.

Entradas	Actividades	Salidas
Lineamientos para la programación de la Oferta Educativa.	Citar a prueba fase I	Registro de citación en el aplicativo de gestión académica.
	Realizar pruebas online y gestionar resultados.	Reporte de seleccionado no seleccionado.
	Generar reporte de preseleccionados.	Reporte de preseleccionado.
	Planear logística Fase II.	Cronograma
	Citar a prueba fase II.	Citación a prueba II
	Reporte de seleccionados.	Reporte seleccionados aplicativo gestión académica.

3. **Matricula:** Se inicia mediante una citación a los aspirantes seleccionados a presentar los documentos requeridos para la matricula.

Entradas	Actividades	Salidas
Calendario Académico para asentamiento de matrícula por programa de formación.	Convocatoria a matricula	Cronograma de citación a matricula.
	Verificación de documento	Lista de chequeo de documentos.
	Asentar matricula	Registro de matrícula en el aplicativo gestión académica.

5.1 GAP análisis

Aplicar el test de preguntas capítulos y controles del Anexo A de la norma ISO COLOMBIANA 27001:2013, a los funcionarios de la oficina de Ingreso.

5.1.1 ANALISIS DEL ANEXO A - ISO 27001:2013

Este análisis, se estableció con relación a los controles definidos en el Anexo A de la norma ISO/IEC 27001:2013.

Para realizar este diagnóstico se utilizó una lista de preguntas con opción de respuesta ‘SI’ o ‘NO’, que fue respondida por funcionarios de las áreas de Ingreso y/o Admisión y Certificación.

A continuación, se relaciona lo resultado de la evaluación de cada uno de los objetivos de control del Anexo A de la norma ISO/IEC 27001:2013:

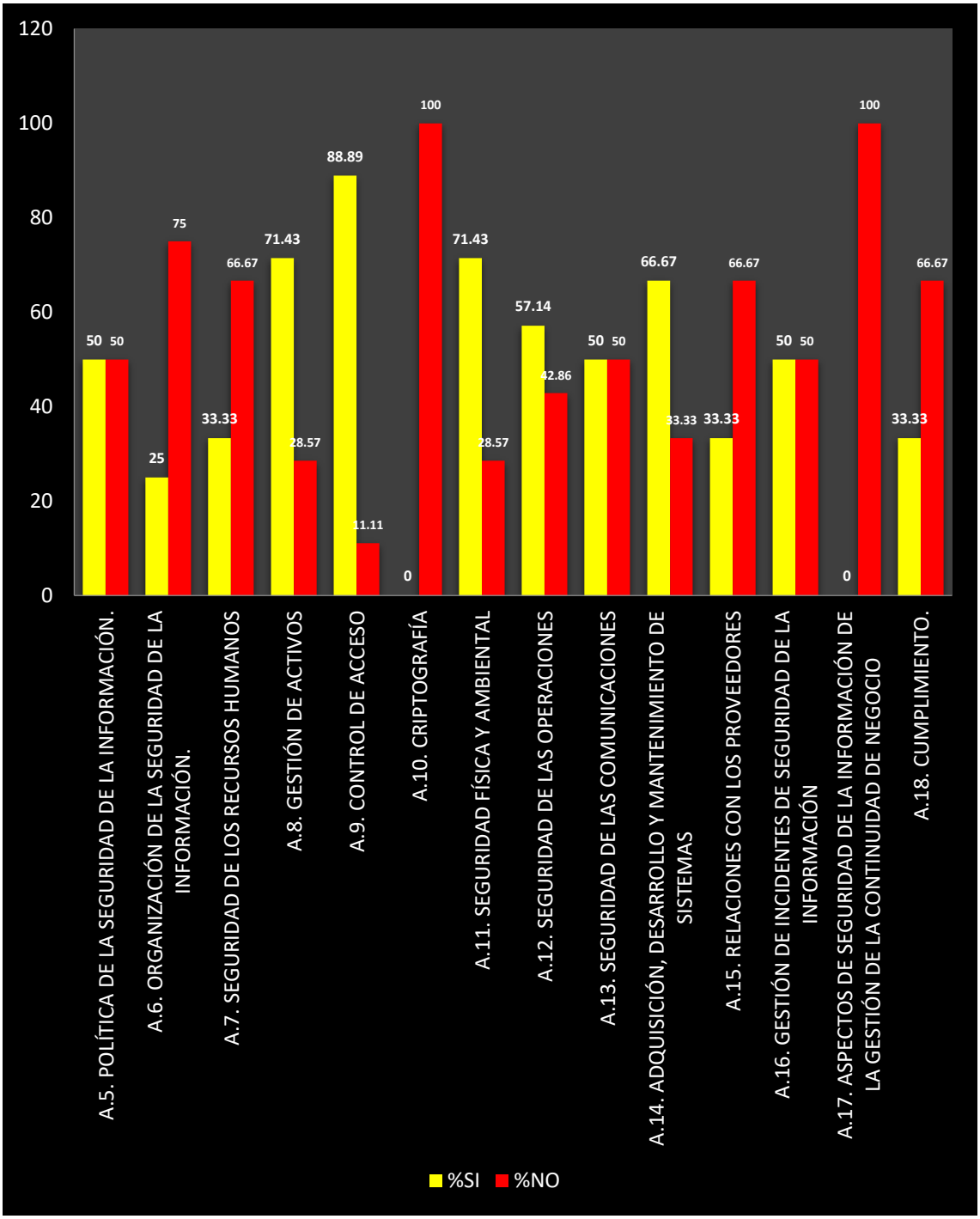

Figura 1. Nivel Cumplimiento Control Anexo A ISO 27001:2013
Fuente: Autor

5.1.2 ANALISIS POR CONTROLES

A continuación, se detalla los controles que tuvieron un cumplimiento por debajo del 40%. Teniendo en cuenta la infraestructura física, tecnológica y presupuestal de la Entidad. Lo anterior basado en la siguiente tabla.

Porcentaje	Valoración
>=56 y <=100%	Alto
>=40% y <=55%	Medio
>=0% y <=39	Bajo

Tabla 1. Valoración de controles.
Fuente: Autor

A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (cumplimiento 25%)

La entidad tiene definidos roles y responsables de la seguridad de la información, pero le falta definir planes para la utilización de dispositivos móviles y el teletrabajo.

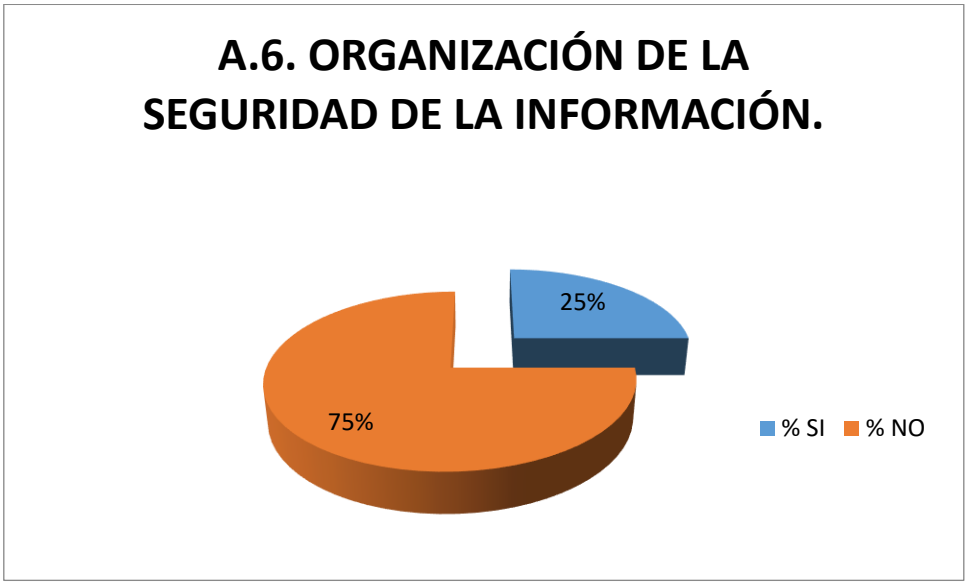

Figura 2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION Anexo A ISO 27001:2013
Fuente: Autor

A.7. SEGURIDAD DE LOS RECURSOS HUMANOS (cumplimiento 33,33%)

No se cuenta con un mecanismo que permite garantizar que los empleados y terceros, estén informados sobre las funciones y las responsabilidades respecto a la seguridad de la información.

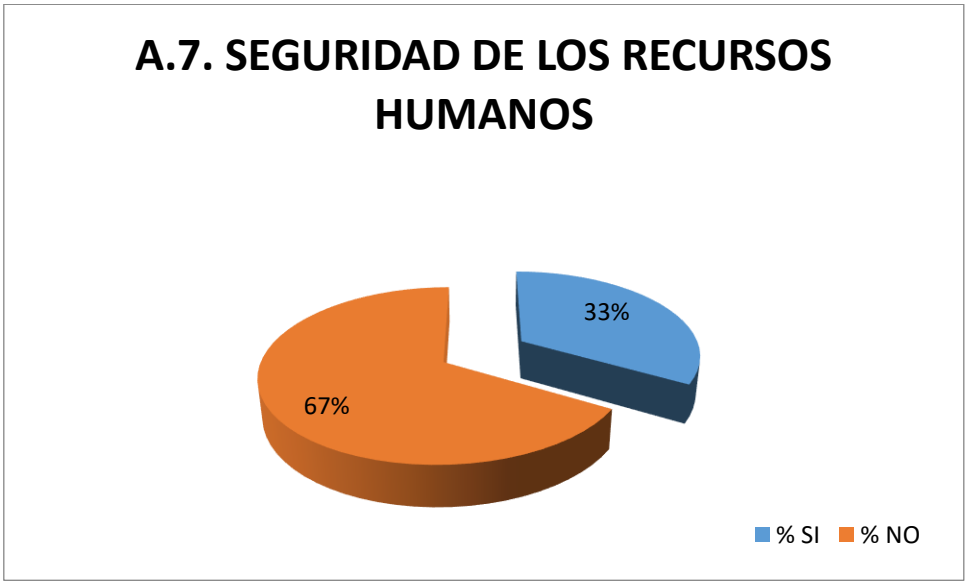

Figura 3. SEGURIDAD DE LOS RECURSOS HUMANOS
Anexo A ISO 27001:2013
Fuente: Autor

A.10. CRIPTOGRAFÍA (cumplimiento 0%)

La entidad no cuenta con mecanismos de cifrado para proteger la información en tránsito y/o reposo, lo cual representa un riesgo debido que no se garantizar la confidencialidad, integridad, autenticidad de la información que se intercambia entre las áreas o con terceros.

Es menester, que la entidad cuente con mecanismos cifrado/descifrados fiables con el objetivo de asegurar la confidencialidad, autenticidad e integridad de la información.

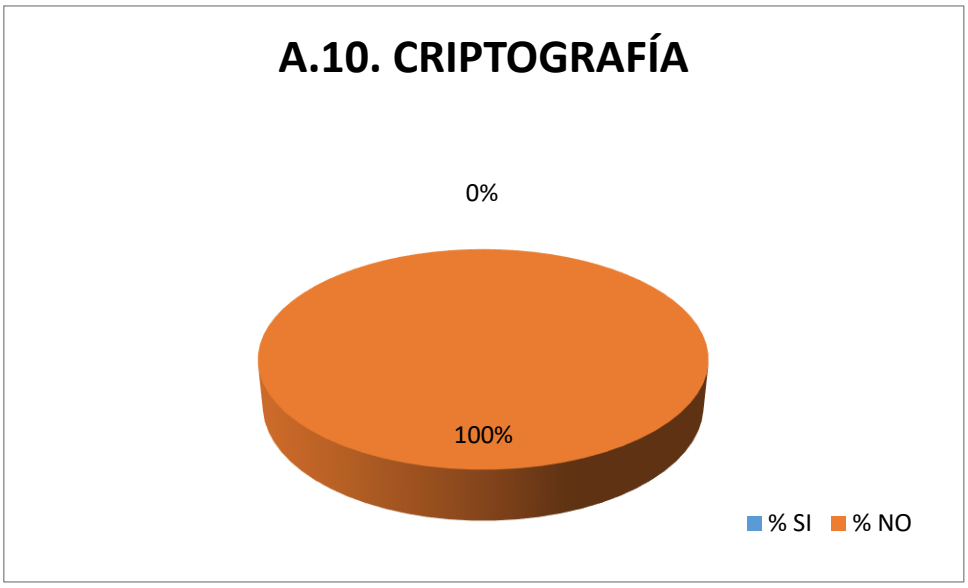

Figura 4. CRIPTOGRAFIA
Anexo A ISO 27001:2013
Fuente: Autor

A.15. RELACIONES CON LOS PROVEEDORES. (Cumplimiento 33,33%)

No existe una política de seguridad en cuanto a los lineamientos de seguridad para la relación con los proveedores con el propósito de evitar accesos no autorizados a la información.

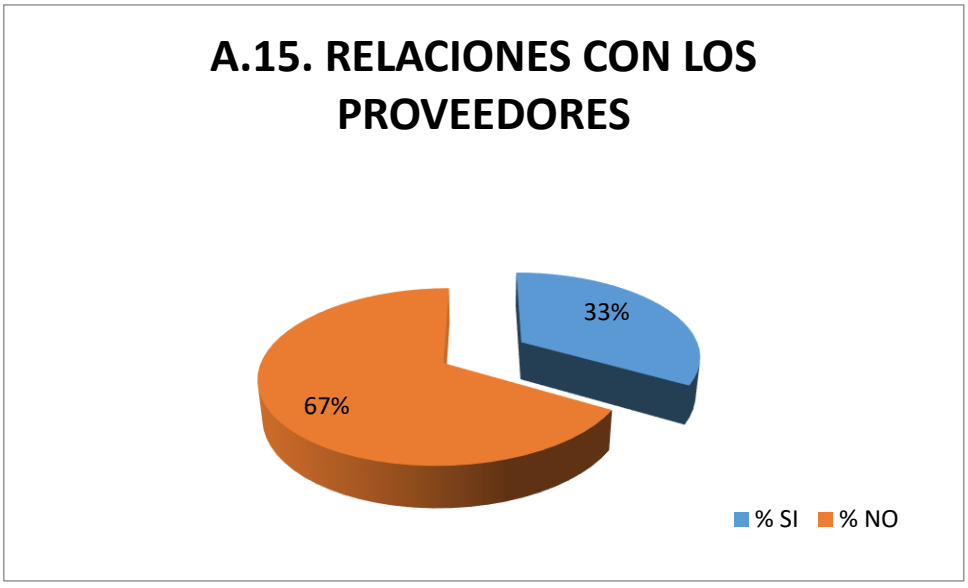

Figura 5. RELACIONES CON LOS PROVEEDORES
Anexo A ISO 27001:2013
Fuente: Autor

A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO. (Cumplimiento 0%)

No se evidencia la seguridad de la información en situaciones adversar que pueden comprometer la disponibilidad de los servicios de Tecnología de Información.

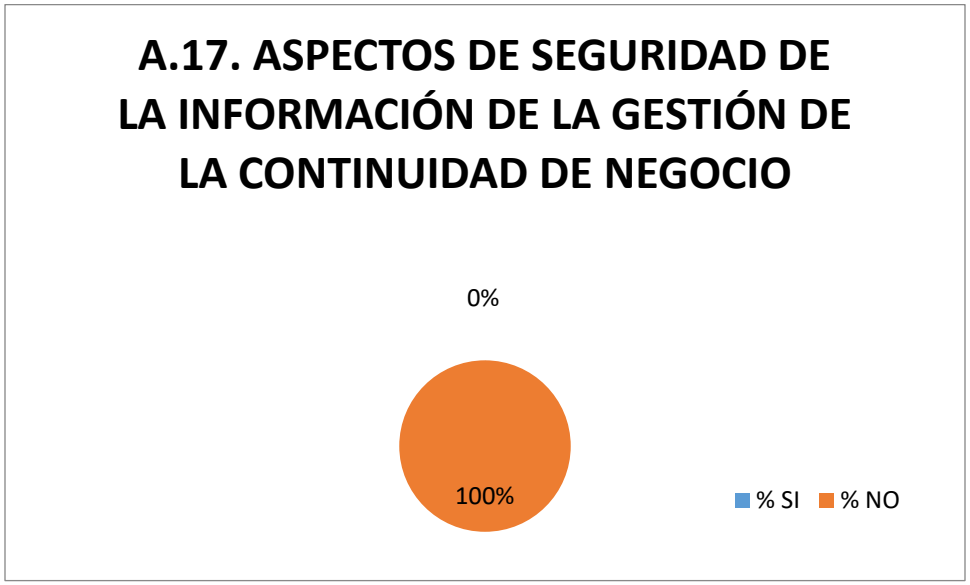

Figura 6. ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DE NEGOCIO
Anexo A ISO 27001:2013
Fuente: Autor

A.18. CUMPLIMIENTO. (Nivel de cumplimiento 33,33)

Debido a que la entidad no cuenta con mecanismo de cifrado/descifrado de la información no cumple con este control.

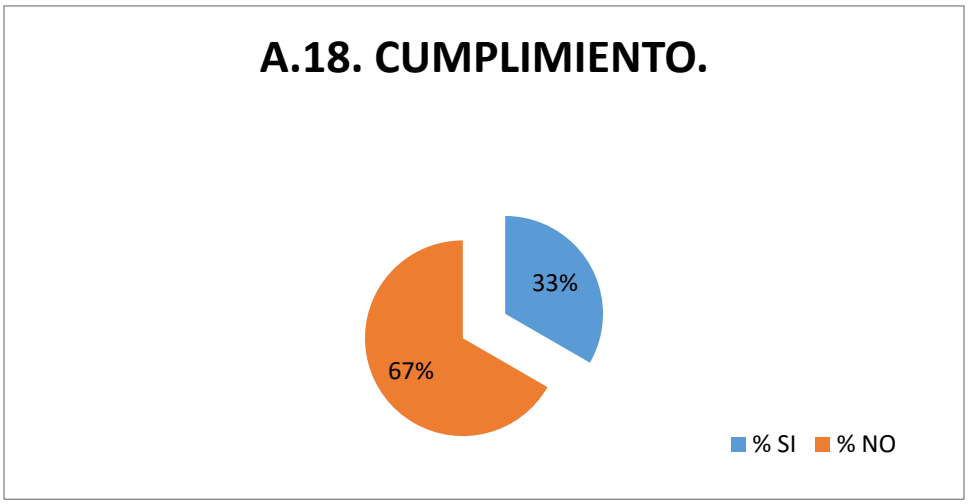

Figura 7. CUMPLIMIENTO
Anexo A ISO 27001:2013
Fuente: Autor

Estado Actual	**Expectativa Futuro**	**Brecha Existente**	**Mejora**
No se han realizado capacitaciones al personal que trabaja en el área de ingreso, en la norma ISO/27001.	Capacitaciones trimestrales de seguridad de la información.	Después del análisis se determinó dos (2) puntos críticos a subsanar. • Personal no capacitado en la norma ISO/27001 • Falta de retroalimentación de los conceptos básicos de la seguridad en la información basados en la norma ISO 27001.	Se realizan recomendaciones de mejora para alcanzar un mejor aprovechamiento de los procesos ya implementados. • Capacitar al personal en las normas de ISO/270001 • Concientizar al personal del uso responsable de usuario y contraseña para el acceso en la plataforma. • Realizar un control donde se verifique el cumplimiento
El acceso al ingreso de la plataforma no es muy seguro, delegación y préstamo de usuarios y contraseñas entre funcionarios.	PC configurados con cuentas estándar para usar y manipular aplicaciones.		

			de los indicadores de implementación de la norma ISO 27001 en la oficina de Ingreso.
Falta de revisiones periódicas al Hardware.	revisiones periódicas del hardware		
Privilegio de administrador activo en los PC, permitiendo instalaciones sin control de aplicaciones.			

5.2 ANALISIS Y EVALUACION DE RIESGO

Tipos de Activos de Información.

La identificación de los activos de información se realizó de acuerdo a las observaciones de campos y entrevista con el personal de las áreas de Ingreso, por lo tanto, se identificaron los activos de información que son utilizados para el desarrollo de las actividades de cada área de la entidad, los cuales fueron el insumo para el proceso de valoración de riesgos.

Activo	Descripción
Aplicaciones	Software de gestión académica Sistemas Operativos Antivirus Navegador web.
Hardware	PC de Escritorio UPS ESTABILIZADORES
Gestión documental	Corresponde a los datos de los procesos.

Valoración de Impacto.

Una vez identificados los activos de información se procedió a valorar su grado de importación y criticidad para la organización.

Aspecto	Criterio	Impacto	Valoración	Escala de Valoración
Financiero	Perdidas económicas	Menor a 200 millones de pesos.	1	Bajo
		Entre 200 millones y 500 millones de pesos.	2	Medio
		Mayor a 500 millones de pesos	3	Alto
Legal	Incumplimiento de	Cancelación del contrato e iniciación del nuevo proceso de contratación.	1	Bajo

	normatividad y legislación,	Afectación a los procesos contractuales.	2	Medio
		Demandas - Desgaste administrativo y financiero	3	Alto
Imagen	Afectación de la imagen institucional a nivel interno y externo.	Pérdida de credibilidad frente a diferentes actores sociales y/o dentro de la Entidad.	1	Bajo
		Afectación a nivel de usuarios internos y/o externos.	2	Medio
		Afectación en la calidad del servicio.	3	Alto

ANÁLISIS DE RIESGO.

A continuación, se presenta la tabla de la calificación de Probabilidad VS Impacto.

Impacto				
		Bajo (1)	**Medio (2)**	**Alto (3)**
Probabilidad	**Bajo (1)**	**1**	**2**	**3**
	Medio (2)	**2**	**4**	**6**
	Alto (3)	**3**	**6**	**9**

	Compromete en un nivel Alto la integridad, confidencialidad y disponibilidad de la información.
	Compromete en un nivel medio la integridad, confidencialidad y disponibilidad de la información.
	No compromete la integridad, confidencialidad y disponibilidad de la información.

Valoración de Probabilidad.

Escala	Probabilidad	Criterio	Frecuencia
1	Baja	El evento puede ocurrir en algún momento.	Una vez en los últimos tres año
2	Media	El evento probablemente ocurrirá en las mayoría de las circunstancia.	Una vez al año
3	Alta	Se espera que el evento ocurra con frecuencia.	Más de una vez por año.

Para la valoración del riesgo y el plan de tratamiento ver el archivo Excel análisis.xls.

5.2.1 VALORACIÓN DE LOS ACTIVOS DE LA INFORMACIÓN.

Cada activo de información tiene una valoración distinta, puesto que cada uno cumple una función diferente en la generación, almacenaje o procesamiento de la información[5].

Disponibilidad- D: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos.

Integridad - I: garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

Confidencialidad - C: aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.

Valor	Disponibilidad
1	Recurso que no puede ser accedido durante un periodo largo de tiempo y que podría ocasionar la detención de las actividades de la empresa.
2	Recurso que no puede ser accedido durante un periodo mediano de tiempo y que podría ocasionar la detención de las actividades de la empresa.
3	Recurso que no puede ser accedido durante un periodo corto de tiempo y que podría ocasionar la detención de las actividades de la empresa.

[5] http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/322__paso_2_valoracin_de_los_activos.html

Valor	Integridad
1	Información cuya modificación sin autorización es posible reparar, pero puede ocasionar un daño sobre las actividades realizadas con el activo.
2	Información cuya modificación sin autorización toma tiempo en exceso en repararse y puede ocasionar un daño en las actividades realizadas con el activo.
3	Información cuya modificación sin autorización es imposible de repararse, deteniendo cualquier actividad dependiendo del activo.

Valor	Confidencialidad
1	Información que puede ser accedida por cualquier funcionario sin necesidad de autorización.
2	Información que solo puede ser accedida por funcionarios.
3	Información que solo puede ser accedida por funcionarios que estén autorizados.

5.3 PLAN DE CAPACITACION DE SEGURIDAD DE LA INFORMACIÓN

La capacitación se llevará a cabo Presencial, en un salón de actividades a través de ayudas visuales y con la contratación de un experto en seguridad de la información.

Actividades:

- Sensibilizar sobre las responsabilidades de los activos de la información a funcionarios, contratistas y personal de apoyo.

- Concientizar a funcionarios, contratistas y personal de apoyo de la entidad de la importancia de la seguridad de la información en cuanto a la confidencialidad, integridad y disponibilidad.
- Sensibilización de los controles de seguridad y la relación que tienen con los activos (Hardware - Software) de la información que manejan.

Folletos pedagógica de Seguridad de la Información

Brindar material de apoyo de seguridad de la información con funcionarios, contratistas y personal de apoyo.

Actividades

- Socializar material educativo de la seguridad informática.
- Administración y buen uso de contraseñas y accesos a los sistemas de información.
- Seguridad de los puestos de trabajo.
- Uso responsable de activos de información (Hardware - Software).
- Cronograma de actividades.
- Análisis de riesgos de los activos de información.

CONCLUSIONES

Enfocada a la Entidad

- La seguridad de la información es una responsabilidad de todos en una entidad que debe estar guiada por manuales y/o procedimientos de buen uso de los activos de información.

- El diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), permitirá identificar amenazas y vulnerabilidades de los activos de información, para posteriormente elaborar plan de tratamientos con la finalidad de mitigar los riesgos.

- Un plan de capacitación y sensibilización sobre seguridad de la información, permitirá crear ambientes de buen manejo y uso de los activos de información.

Enfocado al trabajo de tesis

- La valoración de los riesgos de los activos de información de la oficina de Ingreso del Centro de Educación Técnica y Tecnológica del departamento del Cesar, permitió identificar que el desconocimiento del tema pone en riesgo los procesos que se desarrollan en cuanto a disponibilidad, integridad y confidencialidad.

BIBLIOGRAFÍA

[1] El portal de ISO 27001 en español. [En línea]. Available: http://www.iso27000.es/iso27000.html

[2] ¿Qué es SGSI? [En línea]. Available: http://www.pmg-ssi.com/2015/07/que-es-sgsi/

[3] Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información. [En línea]. https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

[4] Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, TESIS. AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL, 2014, http://repositorio.espam.edu.ec/bitstream/42000/72/1/TESIS%20AMARILIS%20CAROLINA%20LOOR%20P%C3%81RRAGA%20%20VER%C3%93NICA%20ALEXANDRA%20ESPINOZA%20CASTILLO.pdf

ANEXOS

- **Primer Entregable.** Análisis de GAP

  Aplicación de encuesta para determinar el nivel de madurez que presenta la entidad respecto a los temas relacionados con Seguridad de la Información y el nivel de compromisos del personal frente a la confidencialidad, integridad y disponibilidad de los recursos (Hardware - Software) que utiliza. Ver archivo iso.xls.

- **Segundo Entregable.** Metodología de Riesgos de Seguridad de la Información de los activos de información.

  Se utilizó la metodología MAGERIT, a través del cual se clasificaron los activos de la siguiente manera:

  a) Aplicación: Software de gestión académica, sistemas operativos, antivirus, navegadores web.
  b) Hardware: UPS, Estabilizadores, PC de escritorio, Laptop.
  c) Gestión documental: Procesos propias del área de ingreso.

  Una vez se Valoraron los riesgos (impacto y probabilidad) de las amenazas y vulnerabilidades, se diseñó un plan de tratamientos del riesgo. Ver archivo análisis.xls.

- **Tercer Entregable.** Plan de Capacitación y sensibilización de Seguridad de la Información.

  Generar una cultura de seguridad de la información con funcionarios, contratistas y personal de apoyo.

  Actividades

- Sensibilizar sobre las responsabilidades de los activos de la información a funcionarios, contratistas y personal de apoyo.
- Concientizar a funcionarios, contratistas y personal de apoyo de la entidad de la importancia de la seguridad de la información en cuanto a la confidencialidad, integridad y disponibilidad.
- Sensibilización de los controles de seguridad y la relación que tienen con los activos (Hardware - Software) de la información que manejan.

- Administración y buen uso de contraseñas y accesos a los sistemas de información.
- Seguridad de los puestos de trabajo.
- Uso responsable de activos de información (Hardware - Software).
- Cronograma de actividades.
- Análisis de riesgos de los activos de información.

Folletos pedagógica de Seguridad de la Información

Brindar material de apoyo de seguridad de la información con funcionarios, contratistas y personal de apoyo.

Actividades

- Socializar material educativo de la seguridad informática