RESUMEN – TRABAJO DE GRADO

AUTORES	YASMIN MARTINEZ MONCADA ALEJANDRA VERJEL IBAÑEZ JUAN PABLO BACCA MANZANO
FACULTAD	INGENIERÍAS
PLAN DE ESTUDIOS	ESPECIALIZACIÓN AUDITORIA DE SISTEMAS
DIRECTOR	JUAN CAMILO JAIMES FERNANDEZ
TÍTULO DE LA TESIS	DISEÑO DE UNA GUÍA DE BUENAS PRÁCTICAS PARA LA GESTIÓN SEGURA DE LA PLATAFORMA MOODLE DE APOYO A LA PRESENCIALIDAD IMPLEMENTADA EN LA UNIDAD DE EDUCACIÓN VIRTUAL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

RESUMEN
(70 palabras aproximadamente)

EL PRESENTE TRABAJO CONTEMPLA UNA GUÍA DE BUENAS PRÁCTICAS BASADA EN LA NORMA ISO 27002, EN ELLA SE PLANTEAN LOS MECANISMOS Y CONTROLES NECESARIOS PARA LLEVAR A CABO LA GESTIÓN SEGURA DE LA PLATAFORMA MOODLE DE APOYO A LA PRESENCIALIDAD QUE SE MANEJA DESDE LA UNIDAD VIRTUAL; SU PROPÓSITO ES BRINDAR A LA DEPENDENCIA UNA HERRAMIENTA CON LA QUE SEA POSIBLE PROTEGER LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN.

CARACTERÍSTICAS

PÁGINAS: 186	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

DISEÑO DE UNA GUÍA DE BUENAS PRÁCTICAS PARA LA GESTIÓN SEGURA DE LA PLATAFORMA MOODLE DE APOYO A LA PRESENCIALIDAD IMPLEMENTADA EN LA UNIDAD DE EDUCACIÓN VIRTUAL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

ALEJANDRA VERJEL IBAÑEZ
YASMÍN MARTÍNEZ MONCADA
JUAN PABLO BACCA MANZANO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2016

DISEÑO DE UNA GUÍA DE BUENAS PRÁCTICAS PARA LA GESTIÓN SEGURA DE LA PLATAFORMA MOODLE DE APOYO A LA PRESENCIALIDAD IMPLEMENTADA EN LA UNIDAD DE EDUCACIÓN VIRTUAL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

ALEJANDRA VERJEL IBAÑEZ
YASMÍN MARTÍNEZ MONCADA
JUAN PABLO BACCA MANZANO

Trabajo de Grado presentado para optar al título de Especialista en Auditoría de Sistemas

Director
JUAN CAMILO JAIMES FERNÁNDEZ
Esp. Auditoría de Sistemas
Ingeniero de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2016

AGRADECIMIENTOS

En primer lugar queremos agradecer a Dios por permitirnos sonreír ante todos los logros que son el resultado de su ayuda, gracias no solo por estar presente en el camino de nuestra preparación como Auditores, sino también a lo largo de nuestras vidas.

A nuestro director, Esp Juan camilo Jaimes Fernández por el apoyo, la orientación y el respeto a las ideas planteadas para el desarrollo de la investigación.

A nuestros Jurados, las MSc Yegny Karina Amaya y Torcoroma Velásquez Pérez por su tiempo y orientación. Al profesor Mauricio Puentes Velásquez por su confianza, asesoría y apoyo.

Este trabajo con el que culminamos nuestra preparación como especialistas, también es fruto del apoyo que nos brindan las personas que nos estiman, a nuestros familiares y amigos que estuvieron siempre allí, para brindarnos palabras de apoyo en momentos de flaqueza y por alegrase por cada uno de nuestros triunfos, muchas gracias.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE IMÁGENES

ANEXOS

1. DISEÑO DE UNA GUÍA DE BUENAS PRÁCTICAS PARA LA GESTIÓN SEGURA DE LA PLATAFORMA MOODLE DE APOYO A LA PRESENCIALIDAD IMPLEMENTADA EN LA UNIDAD DE EDUCACIÓN VIRTUAL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

1.1. PLANTEAMIENTO DEL PROBLEMA

La mayoría de las empresas utilizan mecanismos para proteger físicamente su infraestructura, inclusive invierten gran cantidad de recursos en la compra de equipos de última tecnología, por lo que asumen que con unas medidas básicas de prevención, la información que se maneja estará segura, esto es un error cuyas consecuencias podrían tener resultados muy negativos, dado que la información es el activo más importante de toda empresa, es imprescindible implementar medidas eficaces que impidan que individuos con malos propósitos intenten comprometer los sistemas informáticos, o que ocurran fallas en la aplicación de medidas de seguridad que atenten contra integridad de la misma.

En la Unidad de Educación Virtual de la Universidad Francisco de Paula Santander Ocaña, se utiliza la plataforma Moodle como apoyo a la presencialidad; según lo observado en esta dependencia, no se cuenta con una guía de buenas prácticas y de controles de gestión de la seguridad de la información que impidan la ejecución de operaciones no seguras y/o no autorizadas sobre la plataforma de apoyo a la presencialidad, que pueden conllevar a daños a los datos y comprometer la confidencialidad, la autenticidad y la integridad de la información.

En la Universidad Francisco de Paula Santander Ocaña, existen unas políticas de seguridad a nivel general para todos los sistemas que se implementan internamente, sin embargo, cada dependencia maneja los procesos de forma diferente por lo que se hace necesario el diseño de una guía de buenas prácticas que se adapte a las necesidades de seguridad específicas de la Unidad de Educación Virtual que permitan una gestión segura de la plataforma de apoyo a la presencialidad basada en Moodle.

1.2. FORMULACIÓN DEL PROBLEMA

¿Con el diseño de una guía de buenas prácticas se garantizará la integridad, confidencialidad y disponibilidad de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual de la Universidad Francisco de Paula Santander Ocaña?

1.3. OBJETIVOS

1.3.1. Objetivo general

Diseñar una guía de buenas prácticas para la gestión segura de la plataforma Moodle de apoyo a la presencialidad implementada en la Unidad de Educación Virtual de la Universidad Francisco de Paula Santander Ocaña.

1.3.2. Objetivos específicos

- Analizar los aspectos administrativos asociados a la seguridad lógica y física de la información gestionada por la Unidad de Educación Virtual a través de la plataforma Moodle de apoyo a la presencialidad para conocer el estado actual de la gestión que se realiza a través de la misma.

- Identificar las vulnerabilidades y amenazas asociadas a los riesgos más representativos de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual para evaluarlos y clasificarlos según su impacto y probabilidad y así establecer mecanismos que permitan contrarrestarlos.

- Determinar prácticas seguras asociadas a los procesos realizados a través de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual, para ofrecer una guía de cómo llevar los procesos de forma segura.

- Estructurar el documento de buenas prácticas que oriente en la gestión de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialdiad en la Unidad de Educación Virtual, para establecer el propósito, recomendaciones y actividades, necesarios de la gestión segura de la información.

1.4. JUSTIFICACIÓN

La información es uno de los activos más importantes de las empresas, el saber administrarla adecuadamente representa una ventaja estratégica frente a otras organizaciones, por ello es importante aplicar controles que garanticen la capacidad de manejar la información de forma segura tanto aquella que se maneja a través de la red como aquellos datos que entran y salen físicamente de la empresa.

En la Unidad de Educación Virtual de la Universidad Francisco de Paula Santander Ocaña, se manejan cursos virtuales, los cuales son utilizados por los docentes como un aporte a la metodología en sus clases presenciales, esta plataforma es conocida como plataforma Moodle de apoyo a la presencialidad, a través de esta, se gestiona toda la información de los cursos (contenidos, usuarios, notas, entre otros) ; dicha información es considerada como uno de los recursos más valiosos de la institución: de una buena gestión de los mismos depende el éxitos, la confiabilidad, autenticidad e integridad de la información contenida en la plataforma.

La administración y gestión de la plataforma de apoyo a la presencialidad se realiza desde la Unidad de Educación Virtual, por esta razón se hace necesario establecer mecanismos que orienten las buenas prácticas en cada uno de los procesos que se llevan a cabo para el manejo de la plataforma y por ende de toda la información que se maneja a través de ella.

El propósito de crear el documento guía de buenas práctica es definir estrategias que permitan potenciar las capacidades de la Unidad Virtual, reducir la vulnerabilidad y limitar las amenazas; al no aplicarlo se seguiría incurriendo en la posibilidad de lidiar

con los impactos negativos de aquellos riesgos que no se puedan contrarrestar, el caso contrario es aquel en el que mediante la implementación de las buenas practicas se realiza una gestión segura de la plataforma Moodle de apoyo a la presencialidad.

1.5. HIPÓTESIS

Con el diseño de una guía de buenas prácticas aplicada a la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual de la Universidad Francisco de Paula Santander Ocaña se optimizará la seguridad en la gestión de la información, de esta manera existirá control sobre todo lo que implique la integridad de la información.

1.6. DELIMITACIONES

1.6.1. GEOGRÁFICAS

Esta investigación se llevará a cabo en el municipio de Ocaña, dentro de la Universidad Francisco de Paula Santander Ocaña, en la dependencia Unidad de Educación Virtual.

1.6.2. TEMPORALES

El tiempo necesario para el desarrollo de esta investigación, será de dos (2) semestres académicos, aproximadamente ocho meses calendario.

1.6.3. CONCEPTUALES

Para el desarrollo de esta investigación se utilizarán ciertos conceptos relacionados con la seguridad de la información, necesarios para entender a cabalidad los temas desarrollados en el proyecto de investigación como el estudio de normas y estándares inherentes a la seguridad de la información y desarrollo de políticas de seguridad.

1.6.4. OPERATIVAS

Las posibles dificultades que se puede encontrar en este proyecto son:

- No encontrar la información completa acerca de la dependencia.

2. MARCO REFERENCIAL

2.1. MARCO HISTÓRICO

La Unidad de Educación Virtual fue creada en junio del año 2013 mediante la resolución No. 0101 como resultado de un proceso de reforma académica y adaptación estratégica a las innovaciones generadas por las nuevas Tecnologías de la Información y la Comunicación (TIC), y de acuerdo a las competencias que se han generado en el mundo moderno, ha querido apropiarse de un modelo de formación virtual, caracterizado por un permanente crecimiento académico, tecnológico y educativo, por la flexibilidad, la autogestión y la interacción con el uso de las Tecnologías, como pilares fundamentales dentro de la oferta académica, siendo así alternativa a la formación presencial y a distancia.

2.1.1. Antecedentes

En la actualidad las nuevas tecnologías mejoran los sistemas de seguridad, pero también hacen más vulnerable la información que se maneja, la seguridad de la información ha tenido que evolucionar y buscar mecanismos que permitan contrarrestar cualquier tipo de mala manipulación de la información.

En Estados Unidos se realizó una investigación en el año 2009 sobre la importancia de asegurar la información en los establecimientos educativos, con esta investigación se exploró el espacio de varios niveles educativos existentes, el aseguramiento de la información y directrices, y la forma en que puede servir como base para ayudar a definir el ámbito de la seguridad de la información, con este trabajo se analizó un punto de partida para la creación de un conjunto adecuado de directrices para el aseguramiento de la información en la educación[1].

En la Colombia existen diferentes establecimientos que buscan cómo crear políticas para el manejo de la información, como en el año 2011 en la Fundación de Educación Superior institución tecnológica San José, en la cual se creó una política pública para la educación virtual en Colombia con la intención de involucrar al Estado en temas públicos para darle solución a un problema o situación que requiere de una intervención especifica en un marco institucional para lograr mitigar el impacto del problema en cuestión o de una situación particular. [2]

En la Universidad Tecnológica de Pereira de Colombia se creó unas políticas de seguridad de activos de la información para presentar la posición de la institución frente a la protección de la información y dar lineamientos para mantener la disponibilidad de la información de acuerdo a las necesidades de continuidad planeadas a nivel de los procesos y por ende de la institución, con esto se logra mitigar cualquier tipo de riesgo que se pueda presentar en la institución y se mantiene de una forma segura la información que allí se maneja.

[1] COOPER, Sthepen, PIOTROWSKI, Victor. An exploration of the current state of information assurance education. 2009.

[2] FUNDACIÓN DE EDUCACIÓN SUPERIOR INSTITUCIÓN TECNOLÓGICA SAN JOSE. La construcción de una política pública para la educación virtual en Colombia. 2011

En el año 2011 en la Universidad Agustiniana se implementó unas políticas de seguridad en la educación virtual, con el objetivo de establecer la política institucional con relación a las dimensiones pedagógica, comunicativa, tecnológica y organizacional propuestas por el Ministerio de Educación Nacional; buscando fortalecer la academia en todos sus niveles y modalidades y garantizando que los procesos de enseñanza-aprendizaje se desarrollen bajo estándares de calidad, equidad, pertinencia y cobertura, de esta manera se estableció la política institucional de Educación Virtual para que se optimice el manejo de la información dentro de esa universidad[3].

Todos estos estudios concluyen en que es muy importante mantener asegurada la información teniendo guías de políticas de seguridad para evitar cualquier manipulación y falta de integridad de este activo tan importante como lo es la información.

2.2. MARCO CONTEXTUAL

Esta guía se desarrollará en la dependencia Unidad de Educación Virtual de la Universidad Francisco de Paula Santander Ocaña, dentro de este contexto se estudiará toda la información con cada una de las personas que hacen parte de esta dependencia, así como analizar todos los aspectos de cada dimensión y sistemas de manejo de información.

2.3. MARCO CONCEPTUAL

2.3.1. Datos[4]

Los datos son en esencia números o texto que puede ser procesado en una computadora, en la actualidad las organizaciones acumulan grandes cantidades de datos en distintos formatos y en distintas bases de datos, entre las que se incluyen datos operacionales o transaccionales en las que se almacenan costos, ventas, inventarios, contabilidad, etc.

2.3.2. Bases de datos[5]

Una base de datos es un sistema computarizado para lleva registros, es posible considerar a la propia base de datos como una especie de armario electrónico para archivar, es decir, es un depósito o contenedor de una colección de archivos de datos computarizados. Los usuarios del sistema pueden realizar una variedad de operaciones sobre dichos archivos como:

-Agregar nuevos archivos a la base de datos.
-Insertar datos dentro de los archivos existentes.
-Recuperar datos de los archivos existentes.
-Modificar datos de archivos existentes.
-Eliminar datos de los archivos existentes.
-Eliminar archivos existentes de la base de datos.

[3] UNIVERSIDAD AGUSTINIANA. Política Institucional de Educación Virtual. [En línea]. 2011. Disponible en internet: http://virtual.uniagustiniana.edu.co/Politica_Educacion_Virtual_Uniagustiniana.pdf
[4] CALDERÓN MÉNDEZ, Neftalí de Jesús. [En línea]. 2010. [Recuperado el día 16 de junio de 2015] Disponible en internet: http://biblioteca.usac.edu.gt/tesis/08/08_0307_CS.pdf
[5] RUIZ FAUDÓN, Sergio Luis. Introducción a los sistemas de bases de datos.2001.

2.3.3. Información[6]

La información es un conjunto de datos acerca de algún suceso, hecho o fenómeno, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo.
La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre deberá estar apropiadamente protegida.

2.3.4. Sistema de Información[7]

Un Sistema de Información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de información no necesariamente incluye equipo electrónico. Sin embargo en la práctica se utiliza como sinónimo de "sistema de información computarizado".

Los elementos que interactúan entre sí son: el equipo computacional, el recurso humano, los datos o información fuente, programas ejecutados por las computadoras, las telecomunicaciones y los procedimientos de políticas y reglas de operación.

Un Sistema de Información realiza cuatro actividades básicas:
Entrada de información: proceso en el cual el sistema toma los datos que requiere para procesar la información, por medio de estaciones de trabajo, teclado, diskettes, cintas magnéticas, código de barras, etc.

Almacenamiento de información: es una de las actividades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardad en la sesión o proceso anterior.

Procesamiento de la información: esta característica de los sistemas permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general en un año base.
Salida de información: es la capacidad de un SI para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, graficadores, cintas magnéticas, diskettes, la voz, etc.

2.3.5. Seguridad de la Información[8]

[6] THOMPSON, Iván. Definición de Información. [En línea]. 2008. [Recuperado el día 16 de Junio de 2015] Disponible en internet: http://moodle2.unid.edu.mx/dts_cursos_mdl/pos/MD/MM/AM/01/Definicion_de_Informacion.pdf
[7] FERNÁNDEZ, Vicenç. Desarrollo de sistemas de información: una metodología basada en el modelado. 2010
[8] GALINDO, Celvin. Seguridad de la información. La firma electrónica avanzada y su certificación. 2014

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad y la integridad de la misma.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

2.3.6. Guía[9]

Se define como el documento que describe en forma sistemática y metodológica, los objetivos, técnicas y procedimientos de las diferentes herramientas de control, para realizar los estudios, análisis y evaluaciones a las entidades o sujetos de control.

2.3.7. Riesgo[10]

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

2.3.9 Plataformas LMS[11]

Las plataformas LMS son espacios virtuales de aprendizaje orientados a facilitar la experiencia de capacitación a distancia, tanto para instituciones educativas como empresas. LMS es el acrónimo en inglés de Learning Management System, que podría traducirse como sistemas para la gestión de aprendizaje.
Este sistema permite la creación de «aulas virtuales» donde se produce la interacción entre tutores y alumnos. También se pueden hacer evaluaciones, intercambiar archivos y participar en foros y chats, además de otras muchas herramientas adicionales.

2.3.10. Moodle[12]

Moodle es una plataforma de aprendizaje diseñada para proporcionarle a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro para crear ambientes de aprendizaje personalizados.

---

[9] UNIVERIDAD FRANCISCO GAVIDIA. [En línea]. 2010. Disponible en internet: http://ri.ufg.edu.sv/jspui/bitstream/11592/7273/3/658.022-T689g-Capitulo%20II.pdf

[10] MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.2012

[11] UNIVERSIDAD INTERNACIONAL DE VALENCIA. Las plataformas LMS. [En línea]. 2007. Disponible en internet: http://www.apega.org/attachments/article/1056/plataformas_lms.pdf

[12] MOODLE.ORG. [En línea]. 2007. Disponible en internet: https://docs.moodle.org/all/es/Acerca_de_Moodle

2.4. MARCO TEÓRICO

La aplicación de una guía de buenas prácticas contribuye a la gestión segura de los sistemas de información, ya que a través de procedimientos apropiados que se adecúen a determinadas necesidades se logran optimizar los procesos.

Para la construcción de la guía de buenas prácticas se requiere realizar un análisis profundo de todos los factores que intervienen en la ejecución de los procesos.

Según Jorge Burgos Salazar y Pedro G. Campos, para la correcta administración de la seguridad de la información se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos de mayor importancia para la información[13], estos son:

Confidencialidad: Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.

- **Integridad:** Busca asegurar:

  - Que no se realicen modificaciones por personas no autorizadas a los datos o procesos.
  - Que no se realicen modificaciones no autorizadas por personal autorizado a los datos o procesos.
  - Que los datos sean consistentes tanto interna como externamente.

- **Disponibilidad:** Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado.

De igual manera estos requerimientos para la información deben cumplirse al implementar o gestionar plataformas LMS como es el caso de Moodle.

Según la página oficial: Moodle es una plataforma de aprendizaje diseñada para proporcionar a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro para crear ambientes de aprendizaje personalizados. Se puede descargar el programa a un servidor web propio, o pedirle a un Moodle Partners asistencia.

Moodle está construido por el proyecto Moodle, que está dirigido y coordinado por el Cuartel General Moodle, una compañía Australiana de 30 desarrolladores, que está soportada financieramente por una red mundial de cerca de 60 compañías de servicio Moodle Partners (Socios Moodle). [14]

[13] BURGO, Jorge, CAMPOS, Pedro. Modelo Para la Seguridad de la Información en TIC. [En línea]. 2008. Disponible en internet: http://ceur-ws.org/Vol-488/paper13.pdf

[14] MOODLE.ORG. [En línea]. 2007. Disponible en internet: https://docs.moodle.org/all/es/Acerca_de_Moodle

Y cuenta con las siguientes características:

- **Mundialmente probado y de confianza**

Impulsando a decenas de miles de ambientes de aprendizaje globalmente, Moodle tiene la confianza de instituciones y organizaciones grandes y pequeñas, incluyendo a Shell, La Escuela Londinense de Economía (London School of Economics), La Universidad Estatal de Nueva York, Microsoft y la Universidad Abierta del Reino Unido (Open University). El número de usuarios de Moodle a nivel mundial, de más de 65 millones de usuarios, entre usuarios académicos y empresariales, lo convierten en la plataforma de aprendizaje más ampliamente utilizada del mundo.

- **Diseñado para soportar tanto la enseñanza como el aprendizaje**

Con más de 10 años de desarrollo guiado por la pedagogía de constructivismo social, Moodle proporciona un conjunto poderoso de herramientas centradas en el estudiante y ambientes de aprendizaje colaborativo, que le dan poder, tanto a la enseñanza como al aprendizaje.

- **Fácil de usar**

Una interfaz simple, características de arrastrar y soltar, y recursos bien documentados, junto con mejoras continuas en usabilidad, hacen a Moodle fácil de aprender y usar.

- **Gratuito, sin cargos por licenciamiento**

Moodle es proporcionado gratuitamente como programa de Código Abierto, bajo la Licencia Pública General GNU (GNU General Public License). Cualquier persona puede adaptar, extender o Modificar Moodle, tanto para proyectos comerciales como no-comerciales, sin pago de cuotas por licenciamiento, y beneficiarse del costo/beneficio, flexibilidad y otras ventajas de usar Moodle.

- **Siempre actualizado**

La implementación de Moodle en código abierto significa que Moodle es continuamente revisado y mejorado, para adecuarse a las necesidades actuales y cambiantes de sus usuarios.

- **Moodle en su idioma**

Las capacidades multilingües de Moodle aseguran que no haya limitaciones lingüísticas para aprender en línea. La comunidad Moodle ha traducido Moodle a más de 120 idiomas (y siguen aumentando), para que los usuarios puedan adaptar al idioma local o nacional su sitio Moodle, junto con muchos recursos, soporte y discusiones comunitarias disponibles en varios idiomas.

- **Plataforma de aprendizaje todo-en-uno**

Moodle proporciona el conjunto de herramientas más flexible para soportar tanto el aprendizaje mixto (blended learning) como los cursos 100% en línea. Configure Moodle habilitando o deshabilitando características del núcleo, e integre con facilidad todo lo necesario para un curso, empleando su rango muy completo de características incorporadas, integrando herramientas colaborativas externas tales como foros, wikis, chats y blogs.

- **Altamente flexible y completamente personalizable**

Debido a que es Código Abierto, Moodle puede ser personalizado en cualquier forma deseada, para adecuarlo a necesidades individuales. Su configuración modular y diseño inter-operable les permite a los desarrolladores el crear plugins e integrar aplicaciones externas para lograr funcionalidades específicas. Extienda lo que hace Moodle al usar plugins y complementos disponibles libremente.

- **Escalable a cualquier tamaño**

Desde unos cuantos estudiantes hasta millones de usuarios, Moodle puede escalarse para soportar las necesidades, tanto de clases pequeñas, como de grandes organizaciones. Debido a su flexibilidad y escalabilidad, Moodle ha sido adoptado para usarse en educación, negocios, organizaciones no-lucrativas y contextos comunitarios.

- **Robusto, seguro y privado**

Comprometido con el resguardo de la seguridad de los datos y la privacidad del usuario, controles de seguridad que son constantemente actualizados, y habiendo implementado procesos del desarrollo de Moodle y software para protección contra acceso no autorizado, pérdida de datos y mal uso, Moodle puede ser desplegado fácilmente en un servidor, o en una nube segura privada para un completo control.

- **Úselo en cualquier momento, en cualquier lugar, en cualquier dispositivo**

Moodle está basado en web, por lo que puede accederse a él desde cualquier lugar del mundo. Con una interfaz por defecto compatible con dispositivos móviles (que pronto será responsiva) y compatibilidad cruzada con diferentes navegadores de Internet, el contenido en la plataforma Moodle es fácilmente accesible y consistente a lo ancho de diferentes navegadores y dispositivos.

- **Recursos extensos disponibles**

Acceda a una muy detallada documentación de Moodle y foros de usuario en múltiples idiomas (incluyendo Español), contenido y cursos gratuitos compartidos por usuarios de Moodle en todo el mundo, así como cientos de plugins y complementos contribuidos por una gran comunidad global.

- **Respaldado por una comunidad fuerte**

El proyecto Moodle está bien soportado por una comunidad internacional activa, un equipo de desarrolladores dedicados de tiempo completo y una red de Moodle Partners certificados. Impulsado por la colaboración abierta y un gran soporte comunitario, el proyecto continúa logrando rápidas mejoras y reparación de defectos, conversiones principales nuevas liberadas cada seis meses.
Para la construcción de la guía de buenas prácticas una de las normas que orientan en proceso es la ISO 27002 Según Board Briefing On It: 2003 *la* ISO/IEC 27002[15] es el Estándar Internacional que nace bajo la coordinación de dos organizaciones:

ISO: International Organization for Standardization.

IEC: International Electrotechnical Commission.

ISO e IEC han establecido un comité técnico conjunto denominado ISO/IEC JTC1 (ISO/IEC Joint Technical Committee). Este comité trata con todos los asuntos de tecnología de información. La mayoría del trabajo de ISO/IEC JTC1 es hecho por subcomités que tratan con un campo o área en particular. Específicamente el subcomité SC 27 es el que se encarga de las técnicas de seguridad de las tecnologías de información, que es en esencia de lo que trata el Estándar Internacional ISO/IEC 27002 (antiguamente llamado ISO/IEC 17799, pero a partir de julio de 2007, adoptó un nuevo esquema de numeración y actualmente es ISO/IEC 27002).

El ISO/IEC 27002 se refiere a una serie de aspectos sobre la seguridad de las tecnologías de información, entre los que se destacan los siguientes puntos:

- **Evaluación de los riesgos de seguridad:** se deben identificar, cuantificar y priorizar los riesgos.

- **Política de seguridad:** deben haber políticas organizacionales claras y bien definidas que regulen el trabajo que se estará realizando en materia de seguridad de la información.

- **Aspectos organizativos de la seguridad de la información:** cómo se trabajará en la seguridad de la información organizativamente, tanto de manera interna (empleados o personal de la organización) como de forma externa o con respecto a terceros (clientes, proveedores, etc.).

- **Gestión de activos:** se debe tener un completo y actualizado inventario de los activos, su clasificación, quiénes son responsables por los activos, etc.

- **Seguridad ligada a los recursos humanos:** especificar las responsabilidades del personal o recursos humanos de una organización, así como los límites que cada uno de ellos tiene con respecto al acceso y manipulación de la información.

[15] BOARD BRIEFING ON IT. Governance Institute. [En línea]. 2003. Disponible en internet: http://www.oecd.org/site/ictworkshops/year/2006/37599342.pdf

- **Seguridad física y ambiental:** consiste en tener una infraestructura física (instalaciones) y ambiental (temperaturas adecuadas, condiciones ideales de operación ideales) adecuadas de modo que no pongan en riesgo la seguridad de la información.

- **Gestión de comunicaciones y operaciones:** asegurar la operación correcta de cada uno de los procesos, incluyendo las comunicaciones y operaciones que se dan en la organización. Esto también incluye la separación entre los ambientes de desarrollo, de prueba y de operación, para evitar problemas operacionales.

- **Control de acceso:** deben existir medidas adecuadas que controlen el acceso a determinada información, únicamente a las personas que están autorizadas para hacerlo, utilizando autenticaciones, contraseñas, y métodos seguros para controlar el acceso a la información.

- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** consiste en tomar medidas adecuadas para adquirir nuevos sistemas (no aceptar sistemas que no cumplan con los requisitos de calidad adecuados), haciendo también un eficiente desarrollo y mantenimiento de los sistemas.

- **Gestión de incidentes en la seguridad de la información:** los incidentes se pueden dar tarde o temprano, y la organización debe contar con registros y bitácoras para identificar a los causantes y responsables de los incidentes, recopilar evidencias, aprender de los errores para no volverlos a cometer, etc.

- **Gestión de la continuidad del negocio:** se deben tener planes y medidas para hacerle frente a los incidentes, de modo que el negocio pueda continuar en marcha gracias a medidas alternativas para que un incidente no detenga las operaciones por tiempos prolongados, que no se pierda información, que no se estanquen o detengan las ventas o negocios, etc.

- **Cumplimiento:** debe darse el debido cumplimiento a los requisitos legales, como derechos de propiedad intelectual, derecho a la confidencialidad de cierta información, control de auditorías, etc.

2.5. MARCO LEGAL

2.5.1. Ley 527 de 1999

"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan disposiciones"[16].

2.5.2. Ley 1273 de 2009

[16] ALCALDÍA DE BOGOTÁ. [En línea]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

"Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"

Bajo la ley 065 de 1993, se expide el código penitenciario y carcelario, marco normativo en el cual se basa el INPEC para la ejecución de las sanciones penales que no denigre la dignidad humana acorde a la carta magna de los comité de derechos humanos[17].

2.5.3. Norma Técnica Colombiana NTC-ISO/IEC 27000

- **Evaluación y tratamiento del riesgo Evaluación de los riesgos de seguridad**

La evaluación de riesgos debería identificar, cuantificar y priorizar los riesgos frente a los criterios para la aceptación del riesgo y los objetivos pertinentes para la organización. Los resultados deberían guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos. Puede ser necesario llevar a cabo el proceso de evaluación de los riesgos y la selección de controles varias veces para cubrir diferentes partes de la organización o sistemas individuales de información. Es recomendable que la evaluación de riesgos incluya el enfoque sistemático para estimar la magnitud de los riesgos (análisis del riesgo) y el proceso de comparación de los riesgos estimados frente a los criterios de riesgo para determinar la importancia de los riesgos (valoración del riesgo).

Es conveniente realizar periódicamente las evaluaciones de riesgos para abordar los cambios en los requisitos de seguridad y en la situación de riesgo, por ejemplo en activos, amenazas, vulnerabilidades, impactos, valoración del riesgo y cuando se producen cambios significativos. Estas evaluaciones de riesgos se deberían efectuar de forma metódica que puedan producir resultados comparables y reproducibles. La evaluación de los riesgos de seguridad de la información debería tener un alcance definido claramente para que sea eficaz y debería incluir las relaciones con las evaluaciones de riesgos en otras áreas, según sea apropiado. El alcance de la evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil. En la norma ISO/lEC TR 13335-3 (Directrices para la seguridad de la tecnología de la información: técnicas para la gestión de la seguridad de la tecnología de la información) se discuten ejemplos de metodologías para la evaluación del riesgo. Tratamiento de los riesgos de seguridad. Antes de considerar el tratamiento de un riesgo, la organización debería decidir los criterios para determinar si se pueden aceptar o no los riesgos. Los riesgos se pueden aceptar si, por ejemplo, según la evaluación se considera el riesgo bajo o que el costo del tratamiento no es efectivo en términos financieros para la organización. Tales decisiones se deberían registrar. Para cada uno de los riesgos identificados después de la evaluación de riesgos es necesario

[17] ALCALDÍA DE BOGOTÁ. [En línea]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

tomar una decisión para su tratamiento. Las opciones posibles para el tratamiento del riesgo incluyen:

a) Aplicación de los controles apropiados para reducir los riesgos.

b) Aceptación objetiva y con conocimiento de los riesgos, siempre y cuando ellos satisfagan la política de la organización y sus criterios para la aceptación del riesgo.

c) Evitación de los riesgos al no permitir acciones que pudieran hacer que éstos se presentaran.

d) Transferencia de riesgos asociados a otras partes, por ejemplo aseguradores o proveedores.

Para aquellos riesgos en donde la decisión de tratamiento del riesgo ha sido la aplicación de controles apropiados, dichos controles se deberían seleccionar e implementar de modo que satisfagan los requisitos identificados por la evaluación de riesgos. Los controles deberían garantizar la reducción de los riesgos hasta un nivel aceptable teniendo en cuenta los siguientes elementos:

a) Requisitos y restricciones de la legislación y de las regulaciones nacionales e internacionales.

b) Objetivos de la organización.

c) Requisitos y restricciones operativos.

d) Costo de la implementación y la operación con relación a los riesgos que se reducen, y que permanezca proporcional a los requisitos y restricciones de la organización.
e) Necesidad de equilibrar la inversión en la implementación y operación de los controles frente a la probabilidad del daño que resultará debido a las fallas de seguridad.

Los controles se pueden seleccionar a partir de esta norma, de otros conjuntos de controles, o se pueden diseñar controles nuevos que satisfagan las necesidades específicas de la organización. Es necesario reconocer que es posible que algunos controles no se puedan aplicar a todos los sistemas y entornos de información, y pueden no ser viables para todas las organizaciones. A modo de ejemplo, el numeral 10.1.3 describe la forma en que se pueden segregar las funciones para evitar fraude y error. Es posible que las organizaciones pequeñas no puedan segregar todas las funciones y que sean necesarias otras formas de lograr el mismo objetivo de control. En otro ejemplo, el numeral 10.10 describe la forma en que se puede monitorear el uso del sistema y recolectar evidencia. Los controles descritos, como el registro de eventos, pueden entrar en conflicto con la legislación correspondiente, como por ejemplo en la protección de la privacidad para los clientes o en el sitio de trabajo. Los controles de seguridad de la información se deberían tener en cuenta en la especificación de los requisitos de

sistemas y proyectos y en la fase de diseño. De lo contrario, se pueden originar costos adicionales y soluciones menos eficaces y, es posible, en el peor de los casos, la incapacidad de lograr una seguridad adecuada. Se debe recordar que ningún conjunto de controles puede lograr la seguridad completa y que se deberían implementar acciones adicionales de gestión para monitorear, valorar y mejorar la eficiencia y la eficacia de los controles de seguridad para apoyar las metas de la organización. 2.4.2.2 Capítulo 5: Política de seguridad de la información Objetivo: brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes. Las directivas deberían establecer una dirección clara de la política según los objetivos del negocio y demostrar apoyo y compromiso con la seguridad de la información a través de la emisión y el mantenimiento de la política de seguridad de la información en toda la organización.
Documento de la política de seguridad de la información Control. La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes. Guía de implementación. El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

a) Definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.

b) Declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.

c) Estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.
d) Explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización. Incluyendo los siguientes:

Cumplimiento de los requisitos legales, reglamentarios y contractuales. Requisitos de educación, formación y concientización sobre seguridad. Gestión de la continuidad del negocio. Consecuencias de las violaciones de la política de seguridad. Definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información. Referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios. Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

Información adicional. La política de seguridad de la información podría formar parte de un documento de política general. Si la política de seguridad de la información se

distribuye fuera de la organización, es necesario tener cuidado de no divulgar información sensible.

2.5.4. Licencia pública general GNU

Copyright (C) 2007 Free Software Foundation, Inc. http://fsf.org/ Se permite la copia y distribución de copias literales de este documento de licencia, pero cambiándolo no está permitido.

Preámbulo

La Licencia Pública General de GNU es una licencia copyleft libre para software y otros tipos de obras.

Las licencias para la mayoría del software y otros trabajos prácticos están diseñados para quitarle a usted la libertad de compartir y modificar los trabajos. En contraste, la Licencia Pública General de GNU pretende garantizarle la libertad de compartir y modificar todas las versiones de un programa - para asegurarse de que sigue siendo libre software para todos sus usuarios. Nosotros, la Fundación para el Software Libre, usamos la Licencia Pública General GNU para la mayoría de nuestro software; también se aplica a cualquier otro trabajo publicado esta forma por sus autores. Puedes aplicarlo a sus programas, también.

Cuando hablamos de software libre, nos referimos a la libertad, no precio. Nuestras Licencias Públicas Generales están diseñadas para asegurarnos de que usted tener la libertad de distribuir copias de software libre (y cobrar por si lo desea), que reciba el código fuente o que pueda conseguirlo si lo quiere, que puede modificar el software o usar fragmentos de él en nuevos programas libres, y que usted sabe que puede hacer estas cosas.
Para proteger sus derechos, necesitamos evitar que otros le nieguen estos derechos o pedirle que renuncie a los derechos. Por lo tanto, usted tiene ciertas responsabilidades si distribuye copias del software, o si lo modifica: responsabilidades de respetar la libertad de los demás.

Por ejemplo, si distribuye copias de un programa de este tipo, ya sea gratuitamente o por una tarifa, debe transmitir a los destinatarios de la misma libertad que ha recibido. Debe asegurarse de que ellos también reciben o pueden conseguir el código fuente. Y debe mostrarles estas condiciones de forma que conocer sus derechos.

Desarrolladores que utilizan la GNU GPL proteger sus derechos con dos pasos: (1) hacer valer los derechos de autor del software, y (2) le ofrecemos esta licencia que le da permiso legal para copiar, distribuir y / o modificarlo.

Para la protección de los desarrolladores y autores, la GPL explica claramente que no hay ninguna garantía para este software libre. Por y de ambos usuarios amor autores, la GPL requiere que las versiones modificadas serán marcados como cambiado, por lo que sus problemas no se atribuyen erróneamente a autores de versiones anteriores.

Algunos dispositivos están diseñados para negar al usuario para instalar o ejecutar versiones modificadas del software dentro de ellos, aunque el fabricante pueden hacerlo. Esto es fundamentalmente incompatible con el objetivo de la protección de la libertad de los usuarios para cambiar el software. La sistemática patrón de tal abuso se produce en el área de productos para las personas a utilizar, que es precisamente donde es más inaceptable. Por lo tanto, han diseñado esta versión de la GPL para prohibir la práctica para aquellos productos. Si apareciesen problemas similares en otros ámbitos, que estar dispuesto a extender esta disposición a aquellos dominios en futuras versiones de la GPL, según sea necesario para proteger la libertad de los usuarios.

Por último, todo programa está constantemente amenazado por las patentes de software. Los Estados no deben permitir que las patentes restrinjan el desarrollo y el uso de software en ordenadores de uso general, pero en los que lo hacen, queremos evitar el peligro especial que las patentes aplicadas a un programa libre podía hacerla efectiva propietario. Para evitar esto, la GPL asegura que las patentes no se pueden utilizar para hacer que el programa no libre.

Los términos y condiciones para la copia, distribución y seguimiento modificación.

Términos y condiciones

0. Definiciones.

"Esta Licencia" se refiere a la versión 3 de la Licencia Pública General de GNU.

"Derechos de autor" también significa las leyes del derecho de autor como el que se aplican a otros tipos de obras, como las máscaras de semiconductores.

"El Programa" se refiere a cualquier obra sujeta al derecho licenciado bajo este Licencia. Cada concesionario se dirige como "usted". "Licenciatarios" y "Destinatarios" pueden ser personas u organizaciones.

Para "modificar" un trabajo significa copiar o adaptar todo o parte de la obra de un modo que requiera permiso de copyright, que no sea la realización de una copia exacta. El trabajo resultante se denomina "versión modificada" de la trabajo anterior o trabajo "basado en" el trabajo anterior.

Un "trabajo amparado" puede ser tanto el Programa no modificado como un trabajo basado en el Programa.

Para "propagar" un trabajo significa hacer cualquier cosa con él que, sin permiso, que le haga directa o indirectamente responsable de infracción en virtud del derecho de autor aplicable, salvo ejecutarlo en un ordenador o la modificación de una copia privada. Propagación incluye la copia, distribución (con o sin modificaciones), poner a disposición del pública, y en algunos países de otras actividades también.

"Distribuir" un trabajo se entiende cualquier tipo de propagación que permite a otra partes para hacer o recibir copias. La mera interacción con un usuario a través de una red de ordenadores, sin transferir una copia, no está transmitiendo.

Una interfaz de usuario interactiva muestra "Avisos Legales Apropiados" en la medida en que incluye una conveniente y prominente visible cuentan que (1) muestra un anuncio de copyright, y (2) le dice al usuario que no hay ninguna garantía para el trabajo (excepto en la medida en que las garantías se proporcionan), que los licenciatarios pueden transmitir la trabajar bajo esta Licencia, y cómo ver una copia de esta licencia. Si la interfaz presenta una lista de opciones o comandos, tales como un menú, un elemento destacado en la lista cumple con este criterio.

1. Código Fuente.

El "código fuente" de un trabajo se entiende la forma preferida del trabajo para realizar modificaciones a la misma. "Código objeto" se entiende cualquier no-fuente forma de trabajo.

Una "Interfaz Estándar" se refiere a una interfaz que sea es un funcionario estándar definido por un organismo de normalización reconocido, o bien, en el caso de interfaces especificadas para un lenguaje de programación en particular, uno que es ampliamente utilizado entre los desarrolladores que trabajan en ese idioma.

Las "Bibliotecas de Sistema" de un trabajo ejecutable incluyen nada, otra que la obra en su conjunto, que (a) se incluye en la forma normal de envasado de un componente principal, pero que no es parte de ese mayor componente, y (b) sólo sirve para permitir el uso de la obra con principales componentes, o para implementar una interfaz estándar para lo cual una aplicación está disponible al público en forma de código fuente. Un "Mayor Componente", en este contexto, significa un componente esencial (Kernel, sistema de ventanas, y así sucesivamente) del sistema operativo específico en la que se ejecuta el trabajo ejecutable, o un compilador utilizado para producir el trabajo, o un intérprete del código objeto utilizado para ejecutarlo.

La "Fuente Correspondiente" de un trabajo en forma de código objeto significa todo el código fuente necesario para generar, instalar, y (para un ejecutar trabajo) ejecutar el código objeto y modificar el trabajo, incluyendo scripts a controlar esas actividades. Sin embargo, no incluye el trabajo de Las bibliotecas del sistema o herramientas de propósito general o generalmente disponible gratis los programas que se utilizan sin modificaciones en la realización de esas actividades, pero que no forman parte de la obra. Por ejemplo, Fuente Correspondiente incluye los archivos de definición de interfaz asociados con archivos de origen para la obra, y el código fuente de las bibliotecas compartidas y dinámica subprogramas vinculados que el trabajo se ha diseñado específicamente para requerir, como por la comunicación de datos intrínseca o el flujo de control entre los subprogramas y otras partes de la obra.

La Fuente Correspondiente no necesita incluir nada que los usuarios pueden regenerar automáticamente de otras partes de la fuente correspondiente.

La Fuente Correspondiente de un trabajo en código fuente es que mismo trabajo.

2. Permisos básicos.

Se otorgan todos los derechos concedidos en virtud de esta licencia por el término de los derechos de autor en el programa, y son irrevocables siempre que el declaró se cumplen las condiciones. Esta licencia afirma explícitamente su ilimitada el permiso para ejecutar el programa sin modificaciones. El resultado de la ejecución de un trabajo amparado está cubierto por esta licencia sólo si la salida, dada su contenido, constituye un trabajo amparado. Esta Licencia reconoce sus derechos de uso razonable u otro equivalente, según lo dispuesto por la ley de derechos de autor.

Usted puede hacer, ejecutar y difundir trabajos amparados que no lo hace transmitir, sin condiciones, siempre y cuando su licencia de otro modo restos vigente. Usted podrá distribuir trabajos amparados a terceros con el único propósito de que ellos hagan modificaciones exclusivamente para usted, o le proporcionan con instalaciones para ejecutar esos trabajos, siempre que cumpla con los términos de esta Licencia en el transporte de todo el material para el que lo hace no controla los derechos de autor. Aquellos de realizar o ejecutar tanto las obras cubiertas para que usted debe hacerlo exclusivamente en su nombre, bajo su dirección y control, en los términos que les prohíban realizar copias de su material con derechos de autor fuera de su relación con usted.

Transmitir en cualquier otra circunstancia se permite únicamente bajo las condiciones establecidas a continuación. Sub-licencia no está permitido; la sección 10 hace que sea innecesario.

3. Protección de Derechos Legales Usuarios frente a Leyes contra la elusión.

Ningún trabajo amparado debe considerarse parte de un programa tecnológico medir la virtud de cualquier ley aplicable que cumpla las obligaciones que le impone el artículo 11 del tratado de copyright WIPO adoptado el 20 de diciembre de 1996, o leyes similares que prohíben o restringen la burla de tales medidas.

Cuando distribuya un trabajo amparado, renuncia a cualquier poder legal para prohibir elusión de medidas tecnológicas en la medida en dicha elusión se efectúa mediante el ejercicio de los derechos bajo esta Licencia con respecto a la obra cubierta, y usted renuncia cualquier intención de limitar el funcionamiento o modificación de la obra como un medio de hacer cumplir, en contra de la obra de usuarios, sus derechos legales o de terceros para prohibir la burla de medidas tecnológicas.

4. Distribución de copias literales.

Usted podrá distribuir copias literales del código fuente del programa como usted recibirlo, en cualquier medio, siempre que y bien visible publicar apropiadamente en cada copia un anuncio de copyright; mantener intactos todos los avisos que indican que esta licencia y cualquier términos no permisivas agregados de acuerdo con la sección 7

se aplican al código; mantener intactos todos los avisos de la ausencia de cualquier garantía; y dar todo los destinatarios una copia de esta Licencia junto con el programa.

Puede cobrar cualquier precio o ningún precio por cada copia que distribuya, y puede ofrecer apoyo o garantía de protección para un honorario.

5. Distribución de Versiones Modificadas de Código.

Usted podrá distribuir un trabajo basado en el programa, o las modificaciones a producirlo del programa, en forma de código fuente bajo los términos del artículo 4, siempre que usted también cumpla las siguientes condiciones:

a) El trabajo debe incluir avisos destacados indicando que ha modificado, y dando una fecha pertinente.

b) El trabajo debe incluir avisos destacados indicando que se trata de liberados bajo esta Licencia y cualquier condición agregados en la sección 7. Este requisito modifica el requisito de la sección 4 de "Mantener intactos todos los avisos".

c) Debe licenciar toda la obra, en su conjunto, en virtud del presente Licencia a cualquier persona que esté en posesión de una copia. Este Por lo tanto, Licencia se aplicará junto con cualquier sección 7 aplicable términos adicionales, a la totalidad de la obra, y todas sus partes, independientemente de la forma en que se empaquetan. Esta Licencia no permiso para licenciar la obra de cualquier otra manera, pero no es así invalidar dicho permiso si usted ha recibido por separado.

d) Si el trabajo tiene interfaces de usuario interactivos, cada uno debe mostrar Avisos Legales Apropiados; Sin embargo, si el programa tiene interactiva interfaces que no muestran Avisos Legales Apropiados, su trabajo no tiene por qué hacen lo hacen.

Una recopilación de un trabajo amparado con otro separado e independiente obras, que no son por sus extensiones naturales del trabajo amparado, y que no se combinan con ella tal como para formar un programa más grande, en o sobre un volumen de un medio de almacenamiento o distribución, se denomina "Agregado" si la recopilación y su copyright resultante no son utilizado para limitar el acceso o los derechos legales de los usuarios de la compilación más allá de lo que permiten las obras individuales. La inclusión de un trabajo amparado en un agregado no causa esta licencia se aplique a las otras partes del total.

6. Distribución No Fuente.

Usted podrá distribuir un trabajo amparado en forma de código objeto bajo los términos de las secciones 4 y 5, siempre que también las distribuya legible por máquina. Correspondiente en los términos de esta Licencia, en una de las siguientes maneras:

a) Distribuir el código objeto en, o embebido en, un producto físico (Incluyendo medios de distribución físicos), acompañado por el Fuentes Correspondientes en un medio físico duradero habitualmente utilizado para el intercambio de software.

b) Distribuir el código objeto en, o embebido en, un producto físico (Incluyendo un medio de distribución físico), acompañada de una oferta por escrito, válida durante al menos tres años y válida durante el siempre y cuando usted ofrece piezas de repuesto o de atención al cliente para ese producto modelo, para dar cualquier persona que posea el código objeto, ya sea (1) un copia de la Fuente Correspondiente para todo el software en el producto que está cubierta por esta Licencia, en un físico duradero medio utilizado habitualmente para el intercambio de software, por un precio no más que su costo razonable de realizar físicamente presente transporte de la fuente, o (2) acceso para copiar el Fuente Correspondiente desde un servidor de red sin coste.

c) Distribuir copias individuales del código objeto junto con una copia de la oferta escrita para proporcionar la fuente correspondiente. Este alternativa se permite sólo ocasionalmente y no comercial, y sólo si usted recibió el código objeto con tal oferta.

d) Distribuir el código objeto ofreciendo acceso desde un designado lugar (gratuitamente o por un cargo), y ofrecer un acceso equivalente a la Correspondiente Fuente de la misma manera por el mismo lugar sin más carga. Usted no tiene que requiere receptores para copiar el fuente Correspondiente junto con el código objeto. Si el lugar para copiar el código objeto es un servidor de red, la fuente correspondiente puede estar en un servidor diferente (gestionado por usted o un tercero) que soporta instalaciones de copia equivalentes, siempre que mantenga instrucciones claras junto al código objeto diciendo dónde encontrar la fuente correspondiente. Independientemente de qué servidor aloja la fuente correspondiente, usted seguirá obligado a asegurar que es disponibles para tan largo como sea necesario para satisfacer estos requisitos.

e) Distribuir el código objeto mediante la transmisión punto a punto, siempre que informe a otros donde el código objeto y la correspondiente fuente de los trabajos se están ofreciendo al público en general sin cobrar bajo la subsección 6d.

Se excluye una parte separable del código objeto, cuyo código fuente de la fuente correspondiente como una biblioteca de sistema, no tiene que ser incluidos en la transmisión de la obra de código objeto.

Un "Producto de Usuario" es (1) un "producto de consumo", lo que significa que cualquier propiedad personal tangible que se utiliza normalmente para uso personal, familiar, o domésticos, o (2) cualquier cosa diseñada o vendida para su incorporación en una vivienda. Para determinar si un producto es un producto de consumo, los casos dudosos se resolverán en favor de la cobertura. Para una determinada producto recibido por un usuario particular, “utilizado normalmente" se refiere a una uso típico o común de ese tipo de producto, sin importar el estado del usuario particular o de la forma en que el usuario en particular en realidad utiliza o espera o se espera que utilice el producto. Un producto es un producto de consumo independientemente de si el producto tiene sustancial usos comerciales, industriales o no de consumo, a menos que tales usos representen la única forma posible de utilizar el producto.

"Información de instalación" para un Producto de Usuario significa cualquier método, procedimientos, claves de autorización, o cualquier otra información necesaria para

instalar y ejecutar versiones modificadas de un trabajo amparado en ese Producto de Usuario desde una versión modificada de su fuente Correspondiente. La información debe suficiente para asegurar que el funcionamiento continuado del objeto modificado código es en ningún caso impide o interfiere con el solo hecho de la modificación se ha hecho.

Si usted transmite una obra de código objeto bajo esta sección en, o con, o específicamente para su uso en, un producto de usuario, y el transporte se produce como parte de una transacción en la que el derecho de posesión y uso del Producto de Usuario se transfieren al destinatario a perpetuidad o por un plazo fijo (independientemente de cómo se caracteriza la transacción), el Fuente Correspondiente transmitida en virtud de esta sección debe ir acompañada por la Información de la instalación. Pero este requisito no se aplica si ni usted ni ningún tercero retiene la capacidad de instalar modificado el código objeto en el producto de usuario (por ejemplo, la obra tiene ha instalado en la ROM).

El requisito de proporcionar Información de Instalación no incluye un requisito que continúe proporcionando servicios de apoyo, garantía, o actualizaciones para una obra que ha sido modificado o instalado por el destinatario, o para el Producto de Usuario en el que ha sido modificado o instalado. El acceso a una la red puede ser denegado cuando la propia modificación sustancial y afecta negativamente al funcionamiento de la red o viole las reglas y protocolos para la comunicación a través de la red.

La fuente correspondiente de la instalación proporcionado, de acuerdo con esta sección debe estar en un formato que sea públicamente documentado (y con una implementación disponible para el público en forma de código fuente), y debe requerir ninguna clave o contraseña especial para desembalaje, la lectura o copia.

7. Condiciones adicionales.

"Permisos Adicionales" son condicionantes que amplían los términos de esta Licencia permitiendo excepciones a una o más de sus condiciones. Los permisos adicionales que son aplicables a todo el programa deberán ser tratados como si estuviesen incluidos en esta Licencia, en la medida que son válidas bajo la ley aplicable. Si los permisos adicionales aplicarán únicamente a parte del programa, esa parte se puede utilizar por separado en virtud de esos permisos, pero todo el programa sigue gobernado por esta Licencia con independencia de los permisos adicionales.

Cuando distribuya una copia de un trabajo amparado, usted puede opcionalmente eliminar cualquier permiso adicional de esa copia, o de cualquier parte del ello. (Permisos adicionales pueden ser escritos para requerir su propia eliminación en ciertos casos cuando se modifica el trabajo). Usted puede colocar permisos adicionales en material añadido por usted a un trabajo amparado, para los que tiene o puede otorgar un permiso apropiado de derechos de autor.

No obstante cualquier otra disposición de esta Licencia, para el material que añadir a un trabajo amparado, usted puede (si está autorizado por los titulares de derechos de autor de ese material) añadir condiciones a esta Licencia con los términos:

a) Ausencia de garantía o limitación de responsabilidad diferente a la términos de los artículos 15 y 16 de esta Licencia;

b) Obligación de mantener determinados avisos legales razonables o atribuciones de autoría en el material o en la legal apropiada Avisos mostrados por los trabajos que lo contengan;

c) Prohibir la tergiversación del origen de ese material, o requerir que las versiones modificadas de este tipo de material marcados en maneras razonables como diferentes de la versión original;

d) Limitar el uso con fines publicitarios de los nombres de los licenciantes o autores del material;

e) Negarse a ofrecer derechos bajo la ley de marcas para el uso de algunos nombres comerciales, marcas registradas o marcas de servicio;

f) Exigir la indemnización de los licenciantes y autores de ese materiales por cualquier persona que distribuya el material (o versiones modificadas de ella) con obligaciones contractuales de responsabilidad para el receptor, para cualquier responsabilidad que estas obligaciones contractuales impongan directamente sobre los licenciantes y autores.

Todos los demás términos adicionales no-permisivas son considerados "más restricciones "en el sentido del artículo 10. Si el Programa como usted recibido, o cualquier parte de ella, contiene un aviso indicando que es regulado por la presente licencia, junto con un término que es una más restricción, puede eliminar ese plazo. Si un documento de licencia contiene una restricción adicional pero permite la renovación de licencias o transmitir bajo esta Licencia, puede añadir a un material de trabajo amparado rige por los términos de ese documento de licencia, siempre que la restricción adicional hace no sobrevivir como renovación de licencias o de transporte.

Si agrega términos de un trabajo amparado de acuerdo con esta sección, debe colocar, en los archivos de origen pertinentes, una declaración de los términos adicionales que se aplican a esos archivos, o un aviso indicando dónde encontrar los términos aplicables.
Los términos adicionales, permisivos o no permisivos, pueden indicarse en la forma de una licencia por escrito separado, o declarado como excepciones; los requisitos anteriores se aplican en ambos sentidos.

8. Terminación.

Usted no puede distribuir o modificar un trabajo amparado salvo lo expresamente proporcionado bajo esta Licencia. Cualquier intento de otro modo para propagar o modificarlo es nulo, y terminará automáticamente sus derechos bajo esta licencia (incluyendo cualquier patente conseguida bajo la tercera párrafo del artículo 11).

Sin embargo, si usted deja toda violación de esta Licencia, entonces su la licencia de un titular de derechos de autor en particular se restableció (a) provisionalmente, a menos que y hasta que el titular del derecho de autor de manera explícita y finalmente termina

su licencia, y (b) de forma permanente, si el derecho de autor titular no le notificará de la violación por parte de algunos medios razonables antes de los 60 días después de la cesación.

Por otra parte, su licencia de un titular de derechos de autor en particular es restableció de forma permanente si el titular del derecho de autor le notifica de la violación por algún cauce, esta es la primera vez que tiene recibido notificación de violación de esta Licencia (para cualquier trabajo) de ese titular de los derechos de autor, y curar la violación antes de 30 días después su recibo de la notificación.

La terminación de sus derechos bajo esta sección no termina las licencias de terceros que hayan recibido copias o derechos de usted bajo esta Licencia. Si se han terminado sus derechos y no de forma permanente reintegrada, usted no califica para recibir nuevas licencias para el mismo material bajo la sección 10.

9. Aceptación no obligatoria por tenencia de copias.

Usted no está obligado a aceptar esta licencia con el fin de recibir o ejecutar una copia del Programa. Propagación auxiliar de un trabajo amparado que ocurre solamente como consecuencia de la utilización de transmisión peer-to-peer recibir una copia del mismo modo no requiere aceptación. Sin embargo, otra cosa que esta Licencia le concede permiso para propagar o modificar cualquier trabajo amparado. Estas acciones infringen los derechos de autor si lo hace No aceptar esta licencia. Por lo tanto, al modificar o propagar una trabajo amparado, usted indica su aceptación de esta Licencia para poder hacerlo.

10. Herencia automática de licencia para destinatarios.

Cada vez que transmitir un trabajo amparado, el destinatario de forma automática recibe una licencia de los licenciadores originales, para ejecutar, modificar y propagar ese trabajo, sujeto a esta licencia. Usted no es responsable para exigir el cumplimiento por parte de terceros con esta licencia.

Una "transacción de entidad" es una transacción de transferencia de control de un organización, o sustancialmente todos los activos de una, o subdivide una organización, u organizaciones que se fusionan. Si propagación de una cubierta los resultados del trabajo de una transacción de entidad, cada parte en ese transacción que reciba una copia de la obra también recibe lo que sea licencias para el trabajo predecesor de la parte interesada tuvo o pudo dar en el párrafo anterior, además de un derecho a la posesión de la Fuente Correspondiente de la obra de su predecesor en el interés, si el predecesor tiene o puede conseguir con un esfuerzo razonable.

Usted no puede imponer ninguna restricción más sobre el ejercicio de los derechos otorgados o concedidos bajo esta licencia. Por ejemplo, es posible que no imponer una cuota de licencia, derechos u otros cargos por el ejercicio de derechos otorgados bajo esta licencia, y usted no puede iniciar un litigio (Incluyendo una reconvención o contrademanda en un juicio) alegando que cualquier reclamación se infringen patentes

por cambiar, usar, vender, ofrecer en venta o importar el Programa o cualquier parte del mismo.

11. Patentes.

Un "colaborador" es un titular de los derechos que autoriza el uso en virtud de este Licencia del Programa o un trabajo en el que se basa el Programa.

"Las reivindicaciones de patentes esenciales" de un contribuyente son todos los reclamos de patentes propiedad o controlada por el contribuyente, si ya adquirida o adelante adquirida, que hayan sido infringidas de alguna forma permitida por esta Licencia, de hacer, usar o vender la versión en colaboración, pero no incluyen las reclamaciones que se infringieron sólo como consecuencia de la modificación adicional de la versión en colaboración. Por efectos de esta definición, "control" incluye el derecho de conceder sub-licencias de patente de manera compatible con los requisitos de esta Licencia.

Cada colaborador le concede una licencia no exclusiva, mundial, libre de regalías licencia de patente en virtud de las reivindicaciones de patentes esenciales del contribuyente, a hacer, usar, vender, ofrecer en venta, importación y de otra manera ejecutar, modificar y propagar el contenido de su versión en colaboración.

En los siguientes tres párrafos, una "licencia de patente" es cualquier expreso acuerdo o compromiso, sin embargo denominados, por no hacer cumplir una patente (Como un permiso expreso de practicar una patente o de pacto de no demandar por infracción de patente). Para "subvención" una licencia de patente como a un tercero significa llegar a un acuerdo o compromiso que no imponga un ejemplo patentar contra el partido.

Si usted transporta un trabajo amparado, confiando a sabiendas en una licencia de patente, y la Fuente Correspondiente de la obra no está disponible para cualquier persona la copia, de forma gratuita y en los términos de esta Licencia, a través de un servidor de red a disposición del público u otros medios de fácil acceso, entonces debe ya sea (1) causa la Fuente Correspondiente a ser tan disponible, o (2) arreglos para privarse de la prestación del licencia de patente para este trabajo en particular, o (3) organizar, de manera consistente con los requisitos de esta Licencia, para extender la patente licencia para receptores aguas abajo. "A sabiendas que confía" significa que tienes conocimiento efectivo, pero para la licencia de patente, el transporte de la obra amparada en un país, o el uso de su destinatario del trabajo cubierto en un país, infringiría una o más patentes existentes en ese país que tiene razones para creer que son válidos.

Si, en virtud de o en conexión con una sola transacción o arreglo, transmitir o propagar por la adquisición de transporte de un trabajo cubierto, y otorgar una licencia de patente a algunas de las partes la recepción de la obra cubierta que les autorice a utilizar, propagar, modificar o transmitir una copia específica del trabajo amparado, entonces la licencia de patente usted concede se extiende automáticamente a todos los destinatarios de la cubierta trabajar y obras basadas en él.

Una licencia de patente es "discriminatoria" si no incluye dentro del alcance de su cobertura, prohíbe el ejercicio de, o es condicionado a la falta de ejercicio de uno o más de los derechos que son específicamente otorgada bajo esta Licencia. Usted no puede transmitir un cubierto, si usted es parte de un acuerdo con un tercero, que es en el negocio de distribución de software, bajo las cuales usted hace el pago al tercero sobre la base de la extensión de su actividad, y en virtud del cual las subvenciones tercero del partido.

Las partes que recibirían el trabajo cubierto de usted, un discriminatoria licencia de patente (a) en relación con las copias de la obra cubierta transportadas por usted (o copias hechas de esas copias), o (b) principalmente para y en relación con los productos o compilaciones específicas que contendrá el trabajo cubierto, a menos que usted entró en ese arreglo, o se le concedió la licencia de la patente, antes del 28 de marzo de 2007.

Nada en esta licencia se interpretará en el sentido de excluir o limitar ninguna licencia implícita o de otras defensas de las infracciones que pueden de lo contrario estará disponible para usted bajo la ley de patentes aplicable.

12. No condicionamiento de la libertad de terceros.

Si se imponen condiciones (ya sea por orden judicial, acuerdo o de otro modo) que contradigan las condiciones de esta Licencia, no lo hacen le exime de cumplir las condiciones de esta Licencia. Si no puede transmitir un trabajo cubierto de manera que se satisfagan simultáneamente sus obligaciones bajo este Licencia y cualquier otra obligación pertinente entonces, como consecuencia, puede no transmite en absoluto. Por ejemplo, si usted está de acuerdo con los términos que obligará para recoger un canon para su posterior transporte de aquellos a quienes usted transporta el Programa, la única forma en que podría satisfacer tanto a esos términos y esta Licencia sería abstenerse completamente de distribuir el Programa.

13. Uso conjunto con la Licencia GNU Affero General Public License.

No obstante cualquier otra disposición de esta Licencia, usted tiene el permiso para enlazar o combinar cualquier trabajo cubierto con una obra con licencia bajo la versión 3 de la Licencia Pública General Affero GNU en una sola trabajo conjunto, y para transmitir la obra resultante. Los términos de esta Licencia continuará aplicando a la parte que es el trabajo amparado, pero los requisitos especiales de la Licencia Pública General Affero GNU, el artículo 13, en relación con la interacción a través de una red se aplicará a la combinación como tal.

14. Versiones Revisadas de esta Licencia.

La Free Software Foundation puede publicar versiones revisadas y / o nuevas de la Licencia Pública General GNU de vez en cuando. Estas nuevas versiones serán similares en espíritu a la presente versión, pero pueden diferir en detalles para considerar nuevos problemas o preocupaciones.

Cada versión recibe un número de versión que la distingue. Si el Programa especifica que cierta versión numerada de la GNU General Licencia Pública "o cualquier versión posterior" se aplican a él, usted tiene la opción de seguir los términos y condiciones, bien de esa numerada versión o de cualquier versión posterior publicada por la Free Software Fundación. Si el Programa no especifica un número de versión de la GNU General Public License, usted puede elegir cualquier versión publicada por la Free Software Foundation.
Si el Programa especifica que un apoderado puede decidir qué futuro versiones de la Licencia Pública General de GNU se pueden utilizar, ese proxy de declaración pública de aceptación de una versión le autoriza permanentemente para elegir esa versión para el Programa.

Las versiones posteriores de la licencia podrán darle adicional o diferente permisos. Sin embargo, no hay obligaciones adicionales se impondrán sanciones a toda autor o copyright titular como consecuencia de su elección que seguir un última versión.

15. Renuncia de garantía.

No hay garantía para el programa, en la medida en que lo permita la ley aplicable. Excepto cuando se indique por escrito del autor titulares y / u otras partes proporcionan el programa "tal cual" sin garantía de cualquier tipo, expresa o implícitas, incluyendo, pero no limitado a, las garantías de comercialización e idoneidad para un determinado finalidad. El riesgo en cuanto a la calidad y el rendimiento del programa es con usted. Si el programa tiene un error, usted asume el costo de cualquier servicio, reparación o corrección.

16. Limitación de responsabilidad.

En ningún caso, a menos que lo exija la ley aplicable o acordado por escrito voluntad cualquier titular de derechos de autor o cualquier otra parte que modifica y / o transmite el programa como permitido anteriormente, será responsable ante usted por daños, incluyendo cualquier general, especial, accidental o consecuente que resulte de la uso o la imposibilidad de uso del programa (incluyendo pero no limitado a la pérdida de datos o a la generación incorrecta o a pérdidas sufridas por usted o por terceras partes o un fallo del programa para operar con otros programas) incluso si dicho tenedor u otra parte ha sido advertido de la posibilidad de tales daños.

17. La interpretación de las secciones 15 y 16.

Si la renuncia de garantía y limitación de responsabilidad proporcionado anterior no se puede dar efecto legal local de acuerdo a sus términos, la revisión de los tribunales se aplicará la ley local que más se aproxima una renuncia absoluta de toda responsabilidad civil en relación con la Programa, a menos que una garantía o compromiso de responsabilidad acompaña un copia del Programa a cambio de una tarifa.

3. DISEÑO METODOLÓGICO

3.1. TIPO DE INVESTIGACIÓN

Para el desarrollo de este proyecto se utilizará la investigación descriptiva con enfoque cuantitativo.

Descriptivo porque el objetivo principal es conseguir una perspectiva general de un problema o situación. En este caso, se identifican las posibles variables que intervienen y sus relaciones, así como las fuentes de información de problemas o situaciones similares y sus soluciones[18].

Enfoque Cuantitativo dado que se usa la recolección de datos para probar una hipótesis con base en la medición numérica y el análisis estadístico para establecer patrones de comportamiento y probar teorías[19].

3.2. POBLACIÓN Y MUESTRA

Durante el desarrollo de este proyecto de investigación se contará con una población de estudio conformada por el personal administrativo de la dependencia y de la división de sistemas, cuyas funciones están relacionadas con la gestión de la plataforma Moodle de apoyo a la presencialidad.

En la dependencia

- Ing Yegny Karina Amaya Torrado: Coordinadora de la Unidad de Educación Virtual.
- Ing Alejandra Verjel Ibáñez: Administradora de la plataforma.

División de Sistemas

- Ing. Antón García: Coordinador de la División de sistemas.
- Ing. Jhon Vergel coordinador Dimensión Tecnológica.
- Ing. Leonardo Zambrano. Administrador de Telecomunicaciones.
- Ing. Numael Molina. Administrador de servidores y servicios a la web.

Dado que la población es pequeña no se sacará una muestra, por lo tanto se estudiará toda la población involucrada en el proceso como fuente de obtención de información.

[18] UNIVERSIDAD CATÓLICA. Tipos de Investigación según Grado de Profundidad y Complejidad. En línea]. 2012. [Recuperado el día 16 de junio de 2015] Disponible en internet: http://portalweb.ucatolica.edu.co/easyWeb2/files/17_6912_tipos-de-investigacian-.pdf

[19] UNIVERSIDAD AUTÓNOMA DEL ESTADO HIDAGO. Aplicación básica de los métodos científicos. En línea]. 2012. [Recuperado el día 26 de Septiembre de 2015] Disponible en internet: http://www.uaeh.edu.mx/docencia/VI_Presentaciones/licenciatura_en_mercadotecnia/fundamentos_de_metodologia_investigacion/PRES39.pdf

3.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE LA INFORMACIÓN

Fuentes Primarias:

Entrevistas al personal administrativo de la dependencia Unidad de Educación Virtual de la UFPS Ocaña.

Visita de observación y aplicación de instrumentos de recolección de la información en la dependencia Unidad de Educación Virtual de la UFPS Ocaña.

Documentación institucional de la dependencia Unidad de Educación Virtual de la UFPS Ocaña.

Fuentes Secundarias:

Libros relacionados con la auditoria informática, seguridad informática y políticas de seguridad de la información.

Artículos científicos basados en la auditoria informática, seguridad informática y políticas de seguridad de la información.

Leyes, normas y estándares concernientes a las tecnologías de la información, técnicas de seguridad de información y políticas de seguridad e la información.

3.4. PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

En la tabla 1 se observa el objetivo específico, las actividades a realizar y el entregable correspondiente para cumplir con el objetivo de esta investigación.

Tabla 1. Seguimiento Metodológico

Objetivo	Actividades	Entregable
Analizar los aspectos administrativos asociados a la seguridad lógica y física de la información gestionada por la Unidad de Educación Virtual a través de la plataforma Moodle de apoyo a la presencialidad para conocer el estado actual de la gestión que se realiza a través de la misma.	Reunión con la coordinadora de la Unidad de Educación virtual con el propósito de solicitar la información requerida.	Instrumentos de recolección de la información: * Entrevista * Observación * Check List * Encuestas
	Realizar una visita a las instalaciones de la Unidad de educación virtual y observar la manera como son llevados procesos y realizar entrevista a la coordinadora.	
	Aplicar instrumentos de recolección de la información (check list y encuesta).	

	Tabulación de la información recolectada.	
Identificar las vulnerabilidades y amenazas asociadas a los riesgos más representativos de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual para evaluarlos y clasificarlos según su impacto y probabilidad y así establecer mecanismos que permitan contrarrestarlos.	Definir las fortalezas y debilidades.	Matriz DOFA
	Clasificar los riesgos y vulnerabilidades detectadas según su probabilidad y el impacto que podrían tener si llegaran a materializarse.	Matriz para el análisis del riesgo
Determinar prácticas seguras asociadas a los procesos realizados a través de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual, para ofrecer una guía de cómo llevar los procesos de forma segura.	Identificar los dominios de la norma ISO 27002 para aplicar los que tienen relación con la dependencia.	Documento con Evidencias y resultados de pruebas realizadas con simulación de servidor –cliente de la plataforma Moodle.
	Plantear estrategias y controles que permita evitar los riesgos y disminuir el impacto de aquellos que se den.	
	Basados en dominios específicos de la norma ISO 27002, determinar qué acciones deben incluirse en el proceso de la gestión de la información que se maneja a través de la plataforma los cuales permitan garantizar la integridad y disponibilidad de la información.	
Estructurar el documento de buenas prácticas que oriente en la gestión de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialdiad en la Unidad de Educación Virtual, para establecer el propósito, recomendaciones y actividades, necesarios de la gestión segura de la información.	Teniendo en cuenta las necesidades encontradas clasificar los procedimientos llevados a cabo y establecer en un documento una guía buenas prácticas para la gestión segura de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual.	Documento que contiene una Guía de Buenas prácticas para la gestión segura de la plataforma Moodle de apoyo a la presencialidad

Fuente: Autores del Proyecto

Determinación de actividades por fase

Fase 1 (F1):
Análisis los aspectos administrativos asociados a la seguridad lógica y física de la información gestionada por la Unidad de Educación Virtual a través de la plataforma Moodle de apoyo a la presencialidad.

Actividades

- Pactar una reunión con la coordinadora de la Unidad de Educación virtual con el propósito de solicitar la información requerida. **(A1)**
- Realizar una visita a las instalaciones de la Unidad de educación virtual y observar la manera como son llevados procesos y realizar entrevista a la coordinadora. **(A2)**
- Aplicar instrumentos de recolección de la información (check list, encuesta). **(A3)**
- Tabulación de la información recolectada. **(A4)**

Fase 2 (F2):
Análisis de la información recolectada para determinar vulnerabilidades y amenazas asociadas a los riesgos más representativos de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual.

Actividades

- Definir las fortalezas y debilidades. **(A5)**
- Clasificar los riesgos y vulnerabilidades detectadas dependiente de la probabilidad y el impacto que podrían tener. **(A6)**

Fase 3 (F3):
Determinar prácticas seguras asociadas a los procesos realizados a través de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual.

Actividades

- Identificar los dominios de la norma ISO 27002 para aplicar los que tienen relación con la dependencia. **(A7)**
- Plantear estrategias y controles que permita evitar los riesgos y disminuir el impacto de aquellos que se den. **(A8)**
- Basados en dominios específicos de la norma ISO 27002, determinar qué acciones deben incluirse en el proceso de la gestión de la información que se maneja a través de la plataforma los cuales permitan garantizar la integridad y disponibilidad de la información. **(A9).**

Fase 4 (F4):

Estructurar el documento de buenas prácticas que oriente en la gestión de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialdiad en la Unidad de Educación Virtual.

Actividades

- Teniendo en cuenta las necesidades encontradas clasificar los procedimientos llevados a cabo y establecer en un documento una guía buenas prácticas para la gestión segura de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual. **(A10).**

4. PRESENTACIÓN DE RESULTADOS

DISEÑO DE UNA GUÍA DE BUENAS PRÁCTICAS PARA LA GESTIÓN SEGURA DE LA PLATAFORMA MOODLE DE APOYO A LA PRESENCIALIDAD IMPLEMENTADA EN LA UNIDAD DE EDUCACIÓN VIRTUAL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

Esta investigación tuvo como finalidad, diseñar una guía de buenas prácticas para la gestión segura de la plataforma Moodle de apoyo a la presencialidad implementada en la Unidad de Educación Virtual de la Universidad Francisco de Paula Santander Ocaña. Para cumplir este objetivo se realizaron los siguientes pasos:

- Analizar los aspectos administrativos asociados a la seguridad lógica y física de la información gestionada por la Unidad de Educación Virtual a través de la plataforma Moodle de apoyo a la presencialidad para conocer el estado actual de la gestión que se realiza a través de la misma.

- Identificar las vulnerabilidades y amenazas asociadas a los riesgos más representativos de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual para evaluarlos y clasificarlos según su impacto y probabilidad y así establecer mecanismos que permitan contrarrestarlos.

- Determinar prácticas seguras asociadas a los procesos realizados a través de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual, para ofrecer una guía de cómo llevar los procesos de forma segura.

- Estructurar el documento de buenas prácticas que oriente en la gestión de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialdiad en la Unidad de Educación Virtual, para establecer el propósito, recomendaciones y actividades, necesarios de la gestión segura de la información.

4.1. Analizar los aspectos administrativos asociados a la seguridad lógica y física de la información gestionada por la Unidad de Educación Virtual a través de la plataforma Moodle de apoyo a la presencialidad para conocer el estado actual de la gestión que se realiza a través de la misma.

Para dar cumplimiento a este objetivo, se llevó a cabo la creación de los instrumentos de recolección de la información: lista de chequeo, encuesta y entrevista, asimismo se realizó la observación correspondiente a las instalaciones de la Unidad de Educación Virtual, posteriormente se analizó la información recolectada a través de estos instrumentos.

4.1.1. Lista de Chequeo

La lista de chequeo fue dirigida a la administradora de la Plataforma de Apoyo a la Presencialidad

- Ing. Alejandra Verjel Ibañez

Mediante la lista de chequeo se logró verificar que la plataforma se encuentra alojada en los servidores ubicados y gestionados desde la División de Sistemas, asimismo se evidencia que se realizan las respectivas copias de seguridad diarias de la plataforma, así como las copias de los cursos de forma individual, esto fue posible verificarlo, a través del administrador de la misma.

4.1.2. Entrevista

La entrevista estuvo dirigida a la Coordinadora de la Unidad de Educación Virtual:

- Msc. Yegny Karina Amaya Torrado

Por medio de la entrevista se evidenció que actualmente la Unidad de Educación Virtual, tiene la meta de virtualizar 10 % de todos los programas presenciales, es por ello que otra de las herramientas que ofrece la dependencia a los docentes es la posibilidad de solicitar la virtualización de materias específicas, en este caso los contenidos que se suben a los cursos se presentan a través de recursos multimediales organizados por unidades, también se incluyen actividades con sus respectivas guías y rúbricas.

Actualmente se encuentran virtualizadas las materias de Cátedra Institucional para cuatro programas presenciales.

El equipo de trabajo está conformado por 9 funcionarios.

4.1.3. Observación

Con el propósito de recolectar la información inicial para realizar la investigación acerca de la gestión de la plataforma Moodle de apoyo a la presencialidad, se solicitó y se llevó a cabo una reunión con la Coordinadora, la ingeniera Yegny Karina Amaya Torrado, quien nos dio a conocer la siguiente información:

- Dentro de los objetivos de la Unidad Virtual se encuentra la responsabilidad de liderar la estrategia virtual al interior de la institución que permita integrar el uso de las tecnologías de Información y Comunicación (TIC´s) en los procesos académicos, es por ellos que a través de la plataforma se ofrecen espacios a los docentes para que incluyan las TIC como herramienta en su metodología de enseñanza.

  Básicamente esto consiste en que el docente puede solicitar la apertura de cursos por cada uno de las materias a su cargo, en este espacio el podrá subir todos los recursos que considere necesarios para el buen desarrollo de su orientación en clases presenciales, claro está, que el docente debe conocer las normas de derechos de autor para no incurrir en la violación de los mismos.

- Las instalaciones de la dependencia se encuentran ubicada en un bloque de aulas, el cual no es el lugar idóneo, dado que hay mucho flujo de personas, igualmente se observó que las estaciones de trabajo, incluyendo la de la administradora de la plataforma, son abiertos y organizados en dos hileras lo que permite que cualquier persona que pase por el pasillo en medio de estas, pueda observar las pantallas de los equipos y por ende la información manejada a través de los mismos.

- Se observó también que en oficina, la administradora de plataforma atiende a estudiantes y docentes con solicitudes respecto a la plataforma como por ejemplo creación de cursos y matrículas.

4.1.4. Encuesta

La encuesta fue realizada a la siguiente población:

- Ing. Antón García: Coordinador de la División de sistemas.
- Ing. Jhon Vergel coordinador Dimensión Tecnológica.
- Ing. Leonardo Zambrano. Administrador de Telecomunicaciones.
- Ing. Numael Molina. Administrador de servidores y servicios a la web.

Tras analizar la información recolectada a través de la encuesta, se pudo apreciar que el personal encuestado afirma **la existencia de la Política de Seguridad**, sin embargo esto no fue posible comprobarlo, dado que se solicitó, pero no se tuvo acceso a dicho documento por lo que se trabajará como supuesta la existencia de la misma más no de afirmará.
Caso contrario ocurre con el documento Plan de Contingencia, el cual si existen y se encuentra alojado en la página institucional, desde donde fue posible acceder al mismo, sin embargo, según los resultados se concluye que no ha sido estudiada por parte del personal.

En cuanto a las capacitaciones que según los resultados, se realizan frecuentemente solo fue posible comprobar la asistencia al evento nacional Moodle Moot que se realiza una vez por año y al cual asisten unos representantes de la institución.

Figura 1 Conocimiento sobre políticas de seguridad de la información

Fuente: Autores del Proyecto.

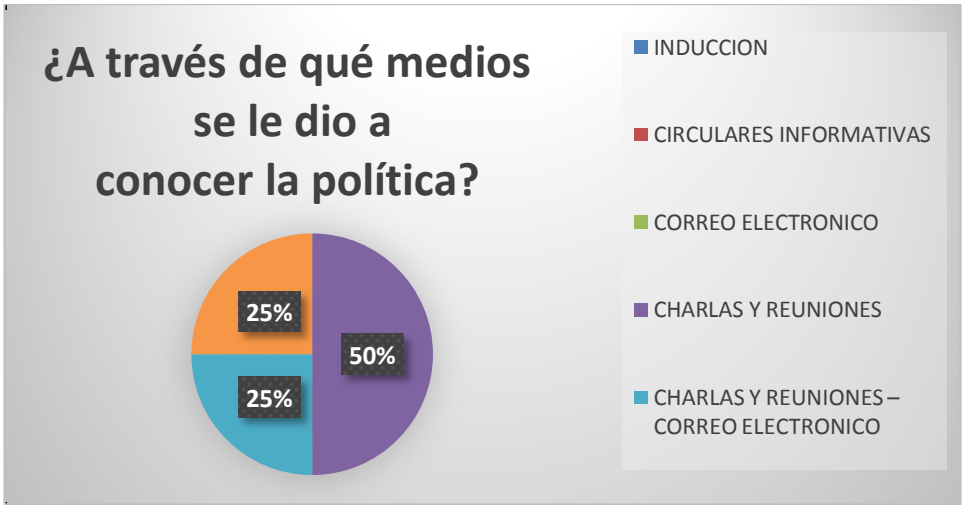
Interpretación: El 100% de las personas encuestadas dicen tener conocimiento sobre las políticas de seguridad de la información, como se observa en la Figura 1. No obstante esta información no pudo ser verificada.

Figura 2 ¿Conoce y entiende la política de seguridad, su propósito e implicaciones?

Fuente: Autores del Proyecto

Interpretación: El 100% de los encuestados dice conocer y entender la política de seguridad, su propósito e implicaciones, como se muestra en la Figura 2.
La población que dice tener conocimiento de la política corresponde al personal encuestado de la División, mientras que la población en estudio restante dice no saber siquiera de su existencia, esto nos lleva a pensar que dicha política no se ha constituido formalmente.

Figura 3 ¿A través de qué medios se le dio a conocer la política?

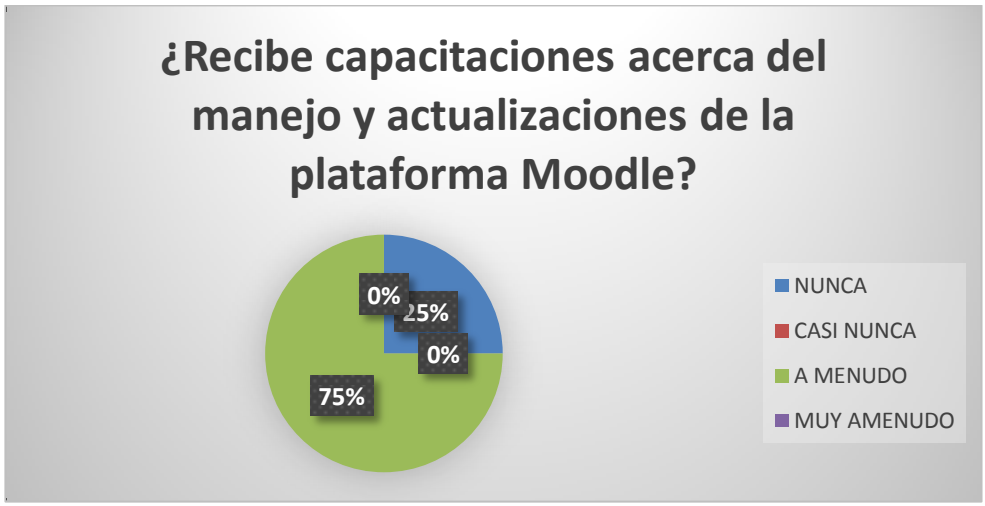


Fuente: Autores del Proyecto

Interpretación: Como se observa en la Figura 3, el medio más utilizado para dar a conocer las Políticas es a través de Charlas y reuniones, sin embargo dado la población

de la Unidad de Educación Virtual dice no haber asistido a ninguna charla al respecto, se presume que se realizan socializaciones internas en la División de Sistemas, más no en la institución en general.

Figura 4 ¿Recibe capacitaciones acerca del manejo y actualizaciones de la plataforma Moodle?



Fuente: Autores del Proyecto

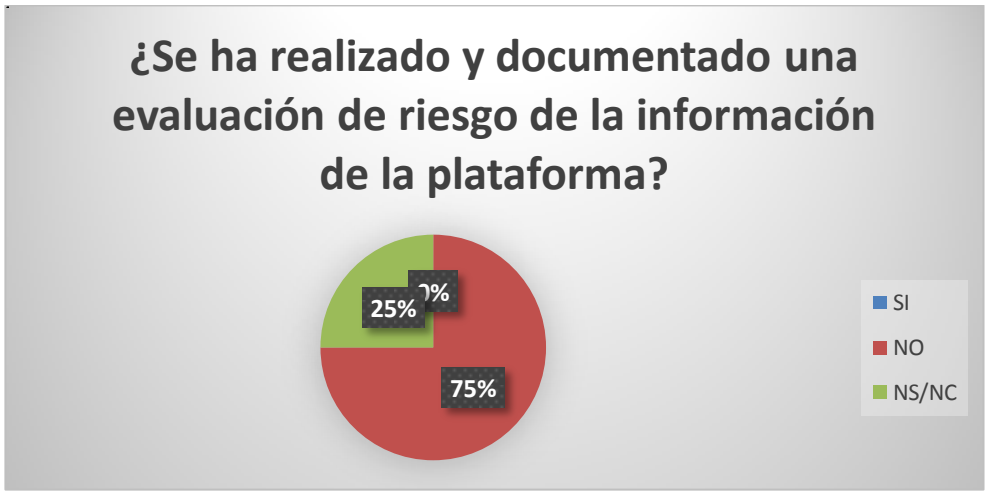
Interpretación: Se observa en la Figura 4, que con un 75% respondieron que a menudo se vienen adelantando capacitaciones sobre el manejo y actualizaciones de la plataforma Moodle seguida de un porcentaje del 25% que dice que nunca. No se obtuvo acceso a actas que den constancia de las mimas por lo que no se pueden comprar las mismas, a excepción del encuentro Nacional Moodle Moot, que se realiza una vez al año.

Figura 5 ¿Existe inventario de activos?

Fuente: Autores del Proyecto

Interpretación: El 100% de los usuarios manifiestan que existe un inventario de activo, tal como lo muestra la Figura 5. No se tuvo acceso ya que esta información es confidencial.

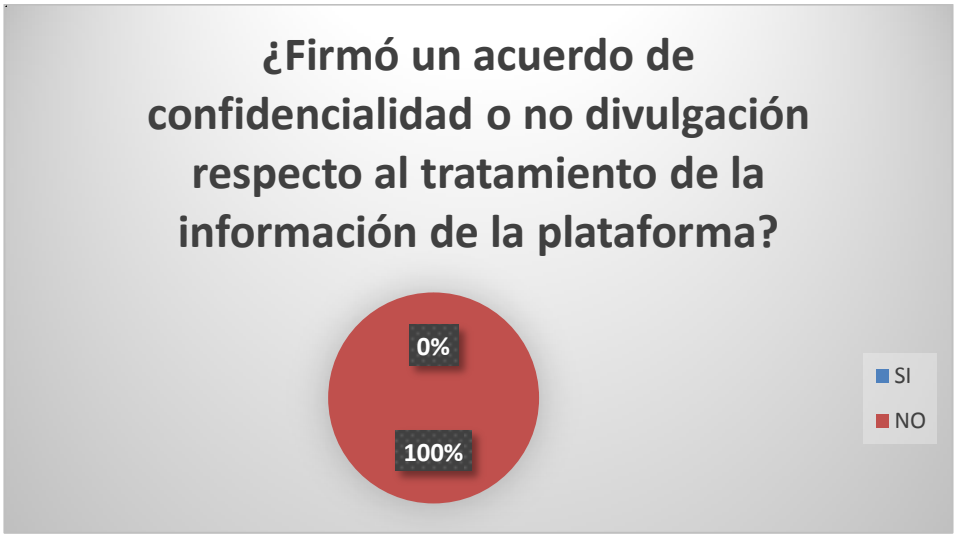
Figura 6 ¿Se ha realizado y documentado una evaluación de riesgo de la información de la plataforma?



Fuente: Autores del Proyecto

Interpretación: El 75% de los encuestados manifiestan que no se ha realizado ni documentado una evaluación de riesgo de la información de la plataforma, el 25% no sabe o no responde, como se observa en la Figura 6.

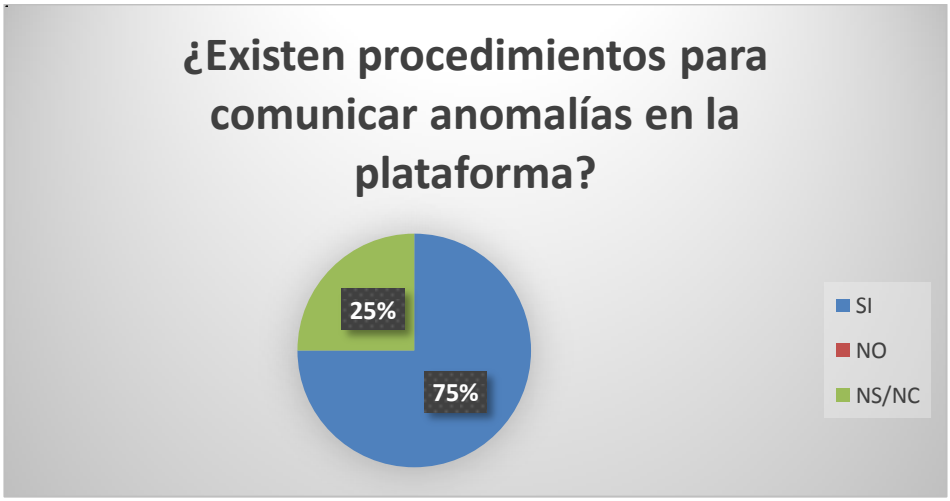
Figura 7 ¿Firmó un acuerdo de confidencialidad o no divulgación respecto al tratamiento de la información de la plataforma?



Fuente: Autores del Proyecto

Interpretación: En la Figura 7, el 100% de los encuestados manifiesta que no firmó un acuerdo de confidencialidad respecto al tratamiento de la información. Sin embargo no se trata de un acuerdo de confiabilidad debidamente establecido, sino una clausula dentro del contrato.

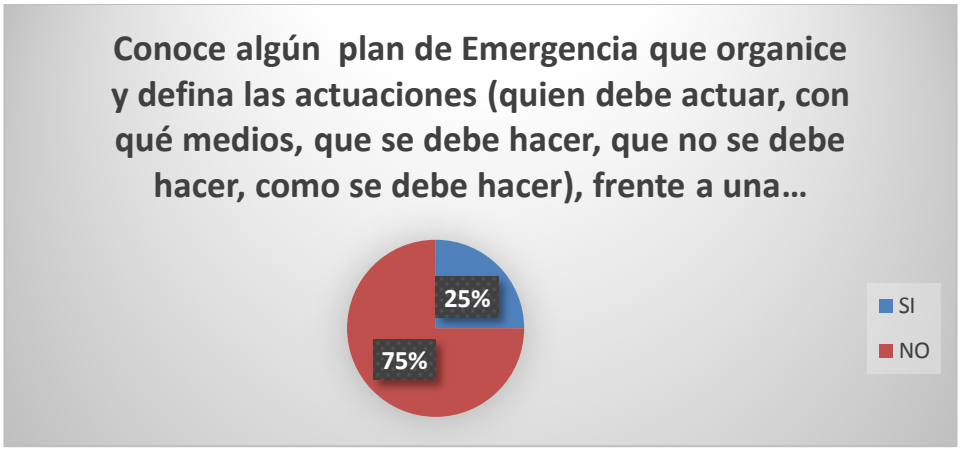
Figura 8 ¿Existen procedimientos para comunicar anomalías en la plataforma?



Fuente: Autores del Proyecto

Interpretación: El 75% de los entrevistados manifestaron que si existen procedimientos para comunicar anomalías en la plataforma, mientras que un 25% manifiesta no saber o no responde, como se observa en la Figura 8. No fue posible verificar la existencia de dichos procedimientos por lo que se presume que si existen no se encuentran documentados.

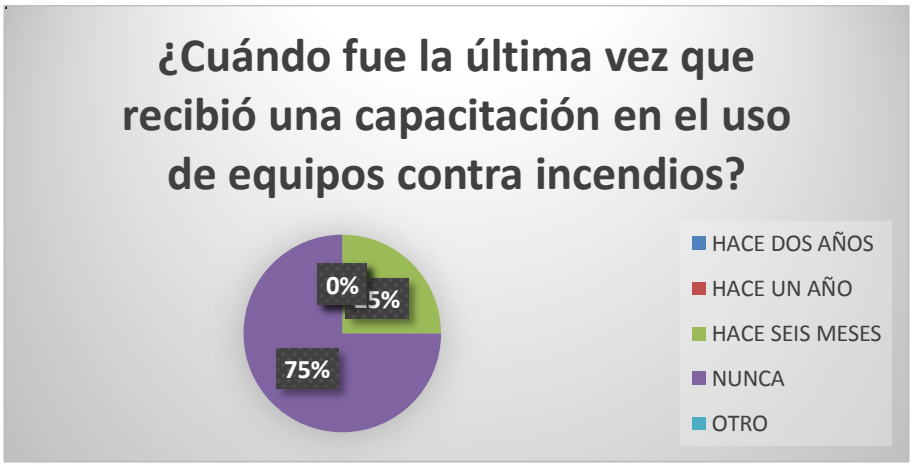
Figura 9 Conoce algún plan de Emergencia que organice y defina las actuaciones (quien debe actuar, con qué medios, que se debe hacer, que no se debe hacer, como se debe hacer), frente a una catástrofe natural que pueda presentarse en la dependencia.



Fuente: Autores del Proyecto

Interpretación: El 75% de las personas NO conocen un plan de emergencia ante posibles fenómenos naturales, como se muestra en la Figura 9, asimismo el 25% manifiesta que SI conoce acerca de un plan de emergencia de estas características.

Figura 10 ¿Cuándo fue la última vez que recibió una capacitación en el uso de equipos contra incendios?

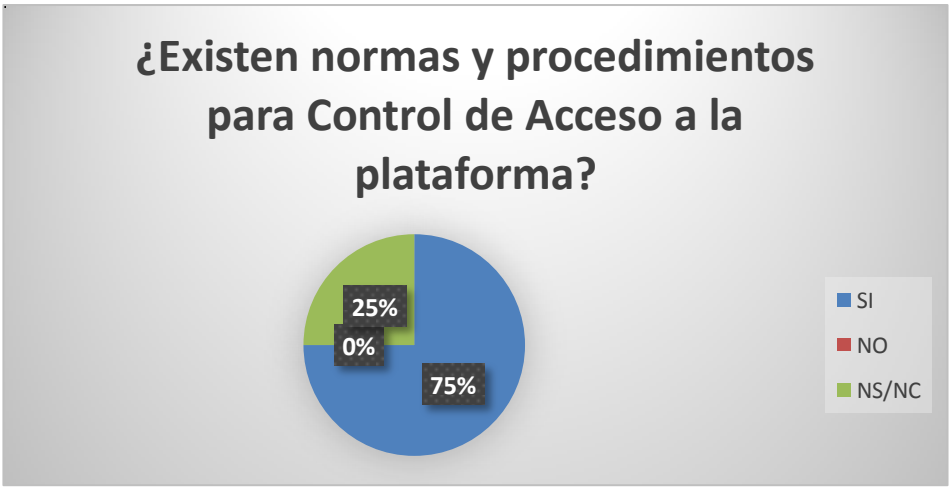


Fuente: Autores del Proyecto

Interpretación: El 75% de los encuestados manifiesta que nunca ha recibido una capacitación sobre el uso de equipos contra incendios, el 25% manifiesta que recibió una capacitación hace seis meses, como se muestra en la Figura 10.

Tras indagar al respecto se puedo concluir que existen brigadas de emergencia en la institución, donde se capacita al personal al respecto, sin embargo una minoría de la población universitaria hace parte de la misma.

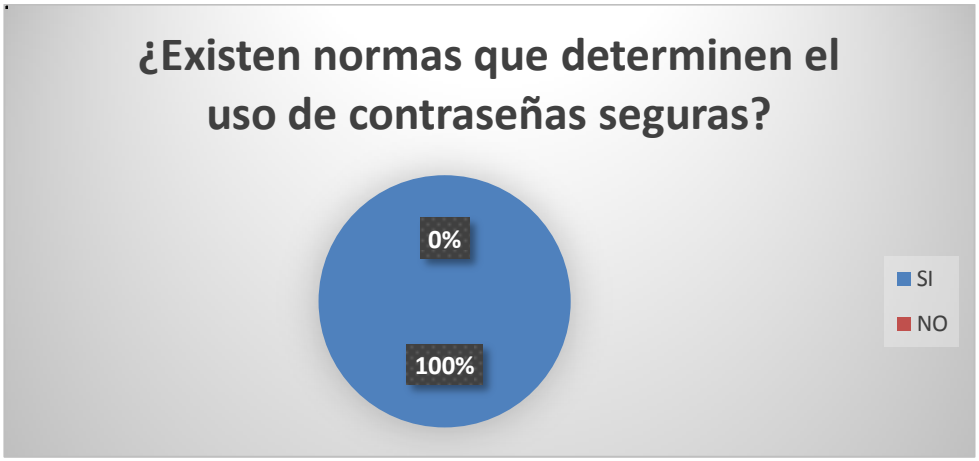
Figura 11 ¿Existen normas y procedimientos para Control de Acceso a la plataforma?



Fuente: Autores del Proyecto

Interpretación: El 75% de los encuestados manifiestan que existen normas y procedimientos para el Control de Acceso a la plataforma, como se observa en la Figura 11, mientras que el 25% manifiesta que No Sabe o No Responde.

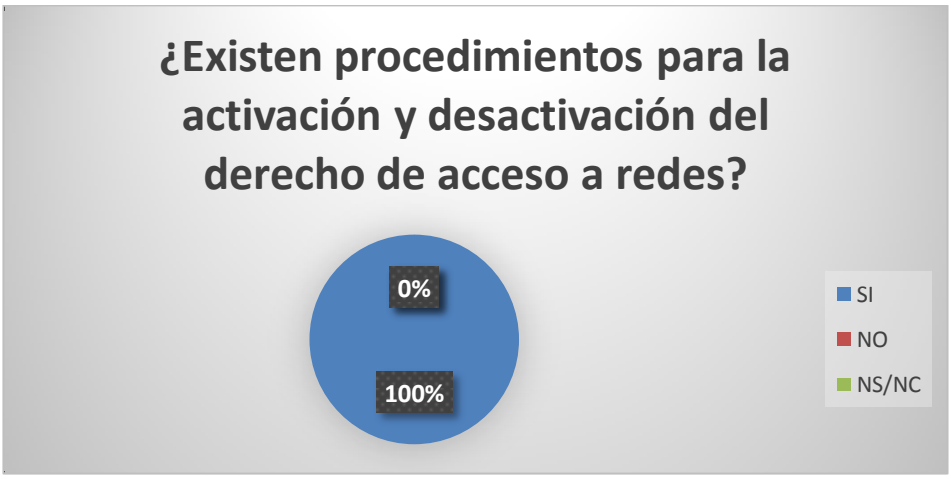
Figura 12 ¿Existen normas que determinen el uso de contraseñas seguras?



Fuente: Autores del Proyecto

Interpretación: El 100% de los usuarios manifiesta que en la actualidad existen normas que determinen el uso de contraseñas seguras, tal como se observa en la Figura 12. Efectivamente si existen normas de contraseñas seguras pero estas se aplican para los sistemas de información incluida la plataforma, sin embargo no para los quipos de las estaciones de trabajo.

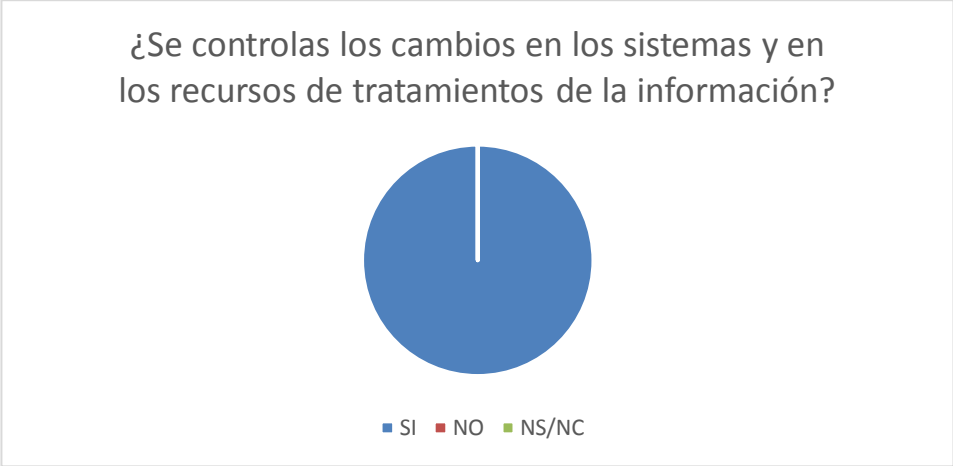
Figura 13 ¿Existen procedimientos para la activación y desactivación del derecho de acceso a redes?



Fuente: Autores del Proyecto

Interpretación: El 100% de los entrevistados manifiestan que existen procedimientos para la activación y desactivación del derecho a redes, como lo muestra la Figura 13.

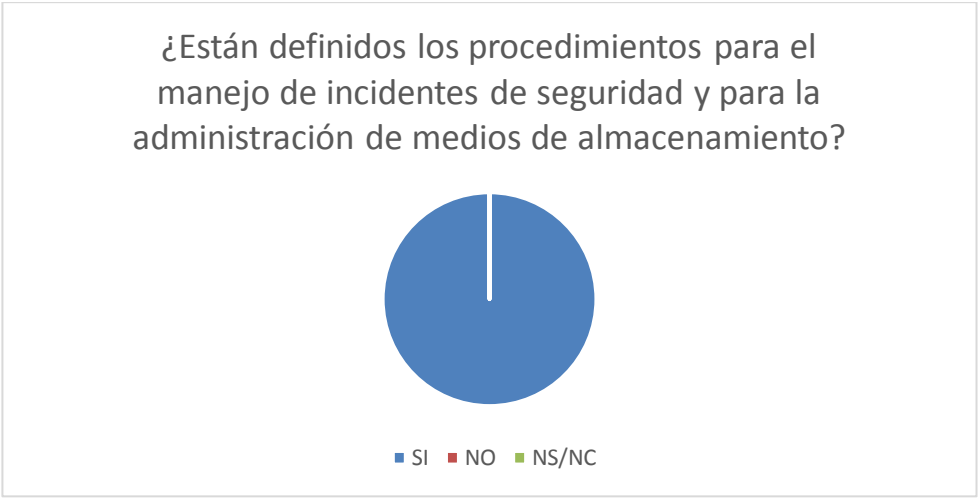
Figura 14 ¿Se controlas los cambios en los sistemas y en los recursos de tratamientos de la información?



Fuente: Autores del Proyecto

Interpretación: El 100% de los entrevistados manifiesta que tiene control sobre los cambios en los sistemas y en los recursos de tratamientos de la información, como se observa en la Figura 14.

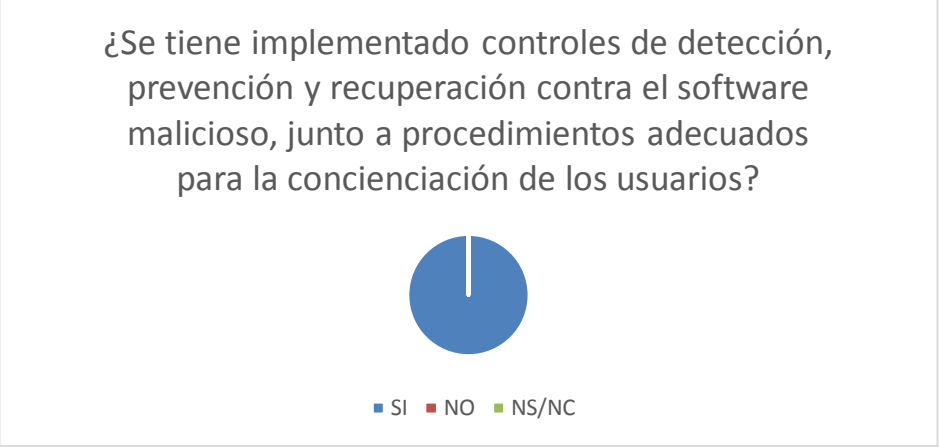
Figura 15 ¿Están definidos los procedimientos para el manejo de incidentes de seguridad y para la administración de medios de almacenamiento?



Fuente: Autores del Proyecto

Interpretación: El 100% de los entrevistados manifiesta que si están definidos los procedimientos para el manejo de incidentes de seguridad y para la administración de medios de almacenamiento, como se observa en la Figura 15.

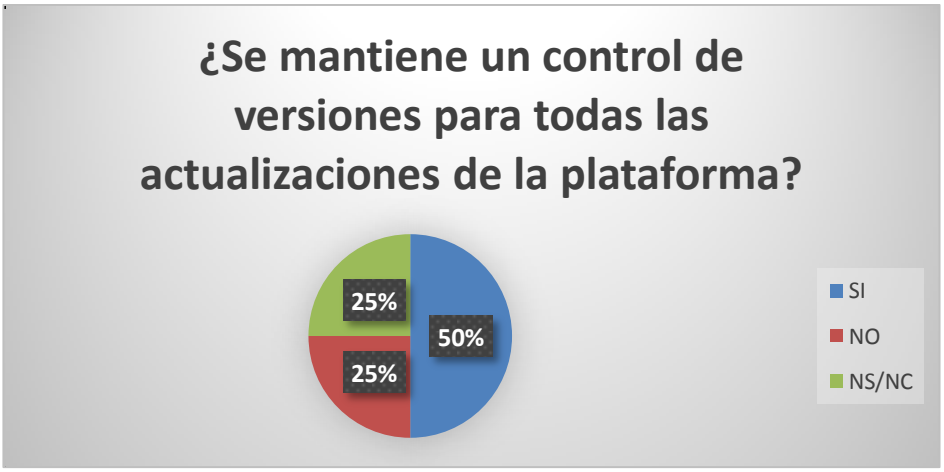
Figura 16 ¿Se tiene implementados controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios?



Fuente: Autores del Proyecto

Interpretación: El 100% de los usuarios manifiesta que tiene implementado controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios, como lo muestra la Figura 16.

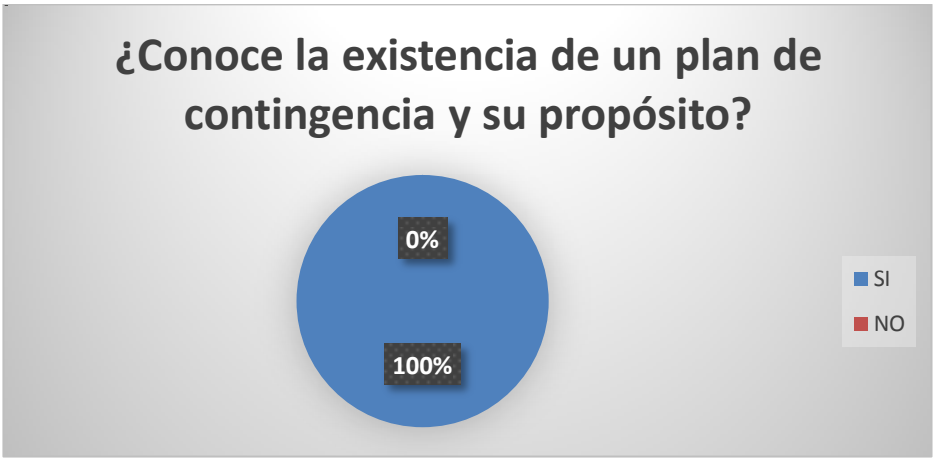
Figura 17 ¿Se mantiene un control de versiones para todas las actualizaciones de la plataforma?



Fuente: Autores del Proyecto

Interpretación: Como se observa en la Figura 17, el 50% de los encuestados manifiesta que SI mantiene un control de versiones para todas las actualizaciones, un 25% manifiesta que NO mantiene un control y otro 25% No Sabe o No responde.

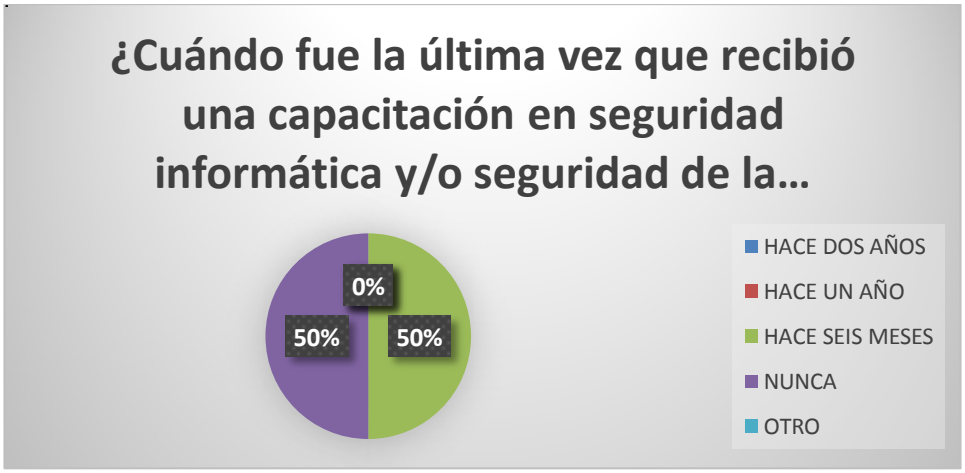
Figura 18 ¿Conoce la existencia de un plan de contingencia y su propósito?



Fuente: Autores del Proyecto

Interpretación: En la Figura 18, el 100% de los entrevistados conoce la existencia de un plan de contingencia y su propósito.
Sin embargo se evidencia que solo se conoce su existencia más no se ha realizado un estudio apropiado del mismo.

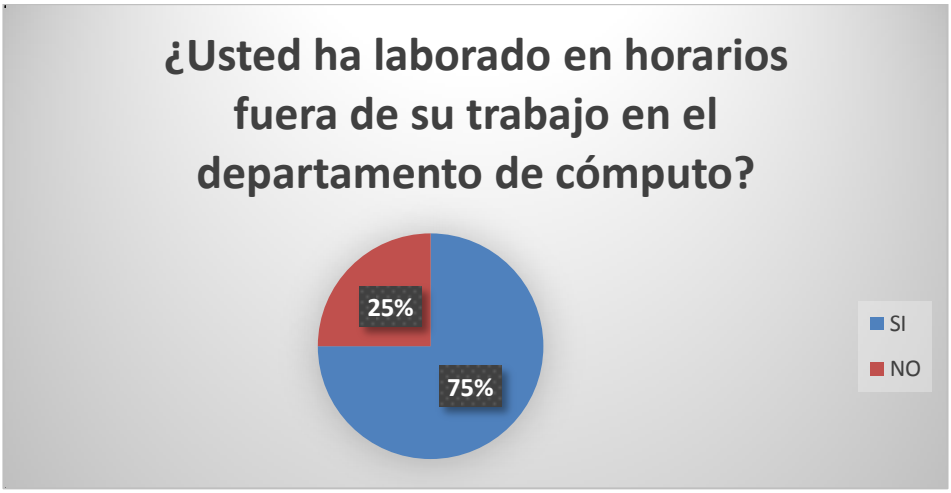
Figura 19 ¿Cuándo fue la última vez que recibió una capacitación en seguridad informática y/o seguridad de la información?



Fuente: Autores del Proyecto

Interpretación: El 50% de los entrevistados manifestaron que hace seis meses fue la última vez que recibieron una capacitación en seguridad informática y/o seguridad de la información, el otro 50% manifiesta que nunca ha tenido este tipo de capacitación, como se observa en la Figura19.

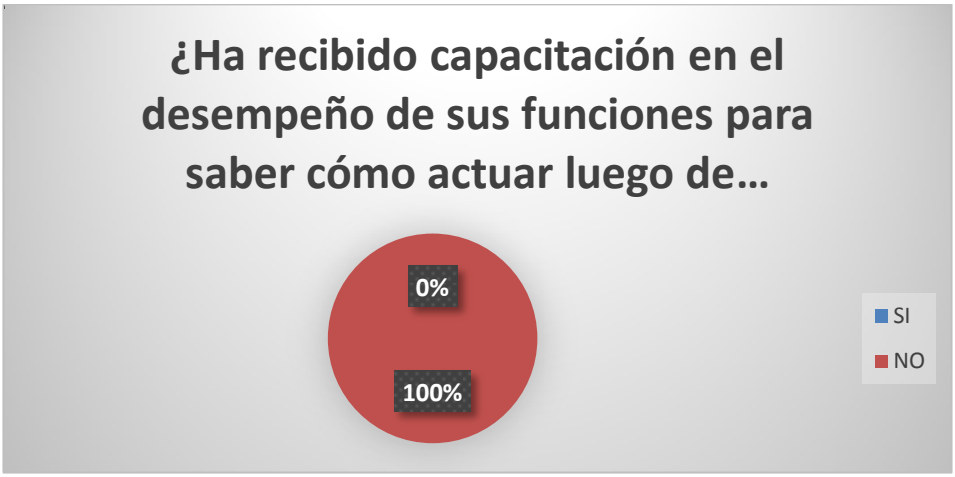
Figura 20 ¿Usted ha laborado en horarios fuera de su trabajo en el departamento de cómputo?



Fuente: Autores del Proyecto

Interpretación: Como se observa en la Figura 20, el 75% de los encuestados manifiesta que ha tenido que trabajar fuera de su horario de trabajo a causa de fallos e incluso falta de tiempo, el 25 % manifiesta que no ha tenido que trabajar fuera de su horario laboral.

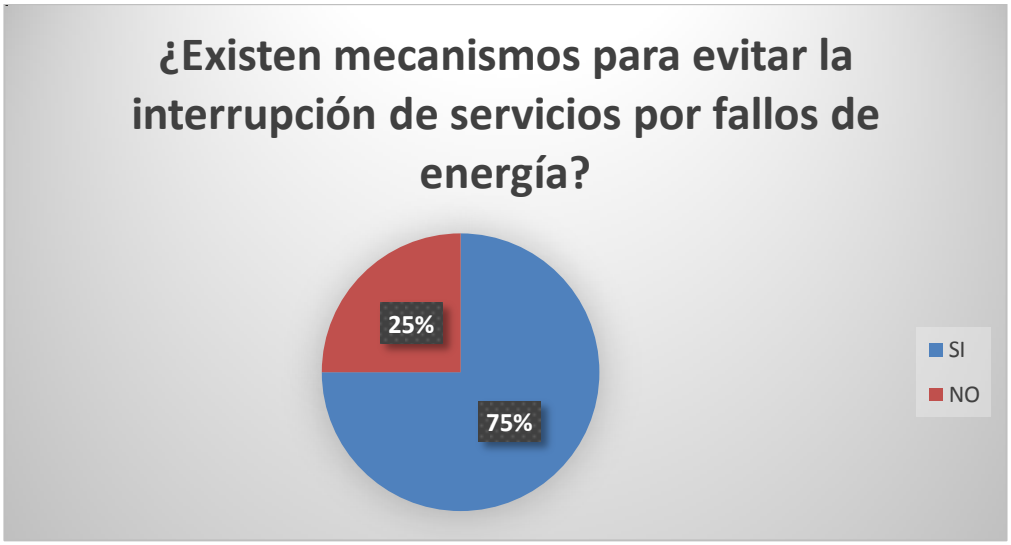
Figura 21 ¿Ha recibido capacitación en el desempeño de sus funciones para saber cómo actuar luego de presentarse incidentes o crisis?



Fuente: Autores del Proyecto

Interpretación: El 100% de los entrevistados manifiesta que ha recibido capacitación en el desempeño de sus funciones para saber cómo actuar luego de presentarse incidentes o crisis, como lo muestra la Figura 21.

Figura 22 ¿Existen mecanismos para evitar la interrupción de servicios por fallos de energía?



Fuente: Autores del Proyecto

Interpretación: El 75% de los encuestados dicen que SI existen mecanismos para evitar la interrupción de servicios por fallos de energía y lo más utilizado son UPS, el 25% manifiesta que no existen estos mecanismos.

4.1.5. Análisis de la información recopilada

Como aspectos a resaltar de la investigación realizada a través de la aplicación de instrumentos se concluye lo siguiente:

El personal encuestado (División de Sistemas) manifiesta conocer sobre la existencia de la política de seguridad, plan de contingencia y demás procedimientos, de la misma manera algunos de ellos afirman que reciben capacitaciones frecuentes sobre los mismos.

Para el caso del resto de la población estudiada, que corresponde al administrador de la plataforma y la coordinadora de la Unidad Virtual, afirman no tener conocimiento acerca de los mismos.

Por esta razón, se procedió a verificar dicha información, para lo cual no se puedo comprobar la existencia de los documentos, a excepción del Plan de Contingencia de TI, en cuanto a las capacitaciones no tuvimos acceso a actas que comprueben las mismas, a excepción del Moodle Moot.

4.2. Identificar las vulnerabilidades y amenazas asociadas a los riesgos más representativos de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual para evaluarlos y clasificarlos según su impacto y probabilidad y así establecer mecanismos que permitan contrarrestarlos.

4.2.1. Matriz DOFA

FA: ¿Cómo aprovechar las fortalezas para minimizar las amenazas?
FO: ¿Cómo usar las fortalezas para aprovechar las oportunidades?
DA: ¿Cómo reducir las debilidades y minimizar las amenazas?
DO: ¿Cómo superar las debilidades aprovechando las oportunidades?

Tabla 2 Matriz DOFA

	FORTALEZAS	**DEBILIDADES**
	F1: Existencia de un plan de contingencia de TI. (L-TT-DSS-002) Rev 2 del 26-06-2015.	**D1:** La inexistencia de un acuerdo formal de confidencialidad.
	F2: Presencia de la dependencia en el evento anual entorno a la plataforma Moodle, (Moodle Moot).	**D2:** Desconocimiento por parte del personal, de las sanciones que acarrean los hechos que atenten contra la confidencialidad, integridad y disponibilidad de la información.
	F3: Existencia de controles de acceso físico al cuarto de servidores en la División de Sistemas.	**D3:** Desconocimiento del Plan de contingencia por parte del personal.
	F4: Existencia de normas que determinan el uso de contraseñas seguras a cualquier sistema de la institución, incluyendo la plataforma Moodle.	**D4:** Desconocimiento de la Política de Seguridad por parte del personal.
	F5: Existencia de controles de detección, prevención y recuperación contra código malicioso (programas antivirus y programas congelador) en la mayoría de equipos.	**D5:** En la Universidad a través de SG-SST se realizan capacitaciones ante emergencias e incidentes, más ninguna de los integrantes de la Unidad Virtual pertenece a dichas brigadas.
	F6: Existencia de documentación de funciones asignadas al personal de la Unidad de	**D6:** No se lleva un control sobre la totalidad de los usuarios que se desvinculan de la

	Educación Virtual. (Estructura Orgánica de la Unidad de Educación Virtual).	institución para eliminar accesos o restringir privilegios.
	F7: Manejo Roles y gestión de privilegios a través de la plataforma Moodle.	**D7:** No se encuentran formalmente establecidos los lineamientos que indiquen a los el tratamiento adecuado de la información a través de la plataforma (derechos de autor, normas)
	F8: Actualizaciones constantes a la plataforma con respaldo es decir, copia de seguridad completa antes de realizar cualquier modificación importante.	**D8:** No se encuentran establecidos formalmente procedimientos para el uso obligatorio de contraseñas seguras en los equipos de las estaciones de trabajo, ni tampoco aquellas para manejo de puestos desatendidos.
	F9: Existencia de control sobre la apertura de espacios para la creación de nuevos cursos en la plataforma Moodle. (Formato F-AC-UEV-002) del 09-10-2015.	**D9:** No se cuenta en la dependencia con mecanismos que permitan apagar de forma segura los equipos de cómputo (UPS) en caso de interrupción de energía eléctrica.
	F10: Se cuenta con servidores de prueba.	**D10:** No se realizan mantenimientos preventivos con la frecuencia necesaria.
	F11: Existencia de la documentación para realizar un análisis de riesgos asociados a equipos de cómputo, comunicaciones (hubs, routers, líneas y teléfonos), información e instalaciones de la institución en general.	**D11:** No se han establecido mecanismos para evaluar que la información montada a plataforma no infrinja los derechos de autor y propiedad intelectual
	F12: Realización periódica de copias de seguridad y almacenamiento seguro de las mismas.	
	F13: capacitación a usuarios en cuanto a la gestión segura de la	

	plataforma según los roles y privilegios asignados.	
	F14: Existencia de una cláusula de confidencialidad dentro de los contratos**.**	
	F15: Capacitación por parte del SG-SST sobre respuestas oportunas emergencias e incidentes.	
OPORTUNIDADES	**ESTRATEGIAS FO**	**ESTRATEGIAS DO**
O1: Se presume la existencia de la Política de seguridad.	Ya que se cuenta con varios mecanismos de seguridad, con ellos es posible actualizar y mejorar la política en caso de que exista o tener pautas para la creación de la misma. **+ F3+F4+F5+F7+F8+F9+ F10+F12 = + O1**	Si se establece una política y se da a conocer al personal, sería ideal para superar muchas debilidades involucradas con la gestión de la información y acciones encaminadas a la protección de la misma. **+O1 = -D1-D2-D3- D4-D6- D8-D9-D10**
O2: Se presume la realización de capacitaciones a cerca de la seguridad de la información y las políticas existentes	En dichas capacitaciones es importante incluir todos los aspectos asociados a la seguridad. **+F1+ F3+F4+F5+F7+ F8+F9+ F10+F12 = + O2**	Mediante capacitaciones se podrá formar al personal para la gestión segura de la información **+O2 = -D2-D3-D4**
O3: Creación del comité de seguridad de la información.		El comité de seguridad se encargaría de verificar que se establecieran mecanismos de seguridad y que los mismos sean llevados a cabo, lo que ayudaría a superar varias de las debilidades existentes. **+O3 = -D2-D3-D4**
O4: Contribuir con el respeto a los derechos de propiedad intelectual y derechos de autor y la confiabilidad de la información montada a plataforma por los usuarios docentes.	Mediante las capacitaciones realizas por la dependencia no solo se enseña a usar la plataforma sino que además se orienta en aspectos de respeto a derechos de autor y temas relacionados. **+F13= +O4**	Dado que la información estructurada por los docentes en la plataforma Moodle e apoyo a la presencialidad no pasa por evaluación previa, esta puede incurrir en violación al derecho de autor, sin embargo a través de las capacitaciones se puede orientar a los docentes

		sobre el tratamiento de la misma. **+O4 = -D11**
O5: Mejorar la calidad de los servicios ofrecidos.	Se pueden aprovechar todas las fortalezas para esta oportunidad. **+(F1-F15) = +O5**	Para mejorar la calidad de los servicios se debe superar las debilidades, con superación de cada una de ellas se mejora cada vez el servicio. **+O = -(D1-D10)**
O6: Respuesta oportuna a incidentes.	Poniendo en práctica el plan de contingencia e incluyendo a personal de la dependencia en las capacitaciones del SG-SST, es posible aprovechar la oportunidad de brindar respuesta oportuna a incidentes. +F1+F15 = +O6	
AMENAZAS	**ESTRATEGIAS FA**	**ESTRATEGIAS DA**
A1: Exposición a la divulgación de información confidencial.	A pesar de no ser suficiente, por lo menos existe dentro de los contratos una cláusula de confidencialidad, lo que indica al empleado su deber de discreción e indica la existencia de sanciones en caso del incumplimiento de la misma. **+F14 = -A1**	Crear acuerdos de confidencialidad los cuales sean firmados por el personal al ingresar a la institución. Realizar periódicamente evaluación de riesgos, llevar registros de ellos y clasificarlos por la magnitud del posible daño. Capacitar al personal periódicamente sobre uso y nuevas versiones de la plataforma. Realizar actualizaciones frecuentes a la política de seguridad existente y dársela a conocer al personal. Dar a conocer al personal el plan de contingencia y realizar capacitaciones constantes.
A2: Posibles daños a equipos y pérdida de información por interrupciones inesperadas de energía eléctrica.	Dado que actualmente no se cuenta con mecanismos que permitan un apagado seguro de los equipos en la dependencia no se puede descartar este riesgo pero es posible mitigar su impacto a través del restablecimiento de las copias de seguridad y la existencia del plan de contingencia siempre y cuando se ponga en práctica. **+F1+F12 = -A2**	
A3: Daños físicos y lógicos	Dentro del plan	

debido a condiciones físicas inapropiadas, falta de mantenimientos.	contingencia se plantea el mantenimiento a equipos, por lo que ya se cuenta con la estratégica, solo falta ponerla en práctica. **+F1 = -A3**	Asignar responsabilidades y privilegios específicos y realizar un control periódico de los mismos.
A4: Posibles afectaciones a la integridad, confidencialidad y disponibilidad de la información por desconocimientos de la política de seguridad y el plan de contingencia.	No existe o no se conoce la política sin embargo a través de otros mecanismos como la asignación de roles y asignación de privilegios es posible mitigarlos. **+F1+F4+F7 = -A4**	
A5: Posibles afectaciones a instalaciones, personal e información en posibles incidentes o desastres naturales debido a la falta de capacitación.	La existencia de brigadas en la universidad gestionadas a través del SG-SST sobre emergencias e incidentes posibilita la capacitación. **+F15 = -A5**	
A6: Posibles accesos a personal no autorizado a la información, cuyas cuentas de usuario continúen activas aún después de haberse desvinculado de la institución.	A través de la gestión de roles y privilegios es posible mitigar este riesgo. **+F7= -A6**	
A7: Posibilidad de acceso ajeno a la dependencia en caso de no asegurar con contraseñas seguras los equipos o no bloquearlo al abandonar momentáneamente la estación de trabajo.	La existencia del plan de contingencia permite contar con la una herramienta para mitigar esta amenaza. **+F1= - A7**	

Fuente: Autores del Proyecto

4.2.2. Matriz de riesgos

Para el análisis de los riesgos se realizaron los siguientes procedimientos:

1) Se analizó la información recolectada y se trató de verificar su veracidad con el propósito de trabajar con información precisa y confiable.

2) Se consultó el análisis de riesgos asociados a la seguridad de :

- En el mobiliarios.
- En el equipo de cómputo en general (procesadores, unidades de disco, impresoras etc.).
- En comunicaciones (hubs, routers, líneas telefónicas).
- Información
- Instalaciones

Establecidos para la institución a través del Plan de Contingencia de TI (L-TT-DSS-002 Rev: B 26-06-2015 14) consultado a través de la página institucional.

3) Se estructuró un listado de riesgos más eminentes detectados en la gestión de la plataforma Moodle de apoyo a la presencialidad desde la Unidad de Educación Virtual de la UFPSO

Tabla 3 Riesgos

Riego	Descripción
R1	Divulgación de información confidencial.
R2	Posibles daños a equipos y pérdida de información por interrupciones inesperadas de energía eléctrica.
R3	Daños físicos y lógicos debido a condiciones físicas inapropiadas, falta de mantenimientos.
R4	Posibles afectaciones a la integridad, confidencialidad y disponibilidad de la información por desconocimientos de la política de seguridad y el plan de contingencia.
R5	Posibles afectaciones a instalaciones, personal e información en posibles incidentes o desastres naturales debido a la falta de capacitación.
R6	Posibles accesos a personal no autorizado a la información, cuyas cuentas de usuario continúen activas aún después de haberse desvinculado de la institución.
R7	Posibilidad de acceso ajeno a la dependencia en caso de no asegurar con contraseñas seguras los equipos o no bloquearlo al abandonar momentáneamente la estación de trabajo (puesto desatendido).
R8	Incursión en violación a derechos de propiedad intelectual y derechos de autor.
R9	Pérdida de información debido a código malicioso debido a desactualización de programas antivirus en aquellos equipos no congelados.
R10	Eliminación insegura de la información.
R11	Borrado accidental de información
R12	Gestión no segura de la información debido a desconocimiento de políticas y procedimientos.

Fuente: Autores del Proyecto

4) Dichos riesgos se clasificaron de acuerdo a su probabilidad e impacto en base a las siguientes escalas tomadas como bases de las siguientes investigaciones.

Color verde: Indica riesgos que tienen una valoración baja

Color amarillo: indican una valoración media.

Color rojo: indican una valoración alta.

* Los estudiantes WILSON ARENALES GONZALEZ y LEIDY JOHANNA AVENDAÑO de la institución universitaria Politécnico Grancolombia

* Los estudiantes JUAN PABLO RODRIGUEZ y LINDA SUSANA VILLA de la universidad de San Buena Aventura.

Arenales González, W., & Avendaño Romero, L. J. (2015). Diseño de un modelo de análisis y diagnóstico del nivel de madurez en si para en mipymes de asesoría legal y oficinas de abogados, como base para la implementación de la norma iso27002

Rodríguez del Valle, J. P., & Villa Jaramillo, L. S. (2013). Administración de riesgo operativo para el área de Contabilidad en Global Securities SA.

Escalas

Tabla 4 Escala de probabilidad

CATEGORÍA	VALOR	DESCRIPCIÓN
INMINENTE	**5**	El riesgo está altamente motivada y es suficientemente capaz de llevarse a cabo y por tanto la materialización de la ocurre diariamente.
FRECUENTE	**4**	La materialización del riego ocurre una vez a la semana.
OCASIONAL	**3**	La materialización del riesgo ocurre una vez al mes.
REMOTO	**2**	La materialización del riesgo ocurre una vez al año.
IMPROBABLE	**1**	El riesgo no posee la suficiente motivación y capacidad o nunca se ha materializado, pero no se descarta su ocurrencia.

Fuente: Autores del Proyecto

Tabla 5 Escala de impactos

CATEGORÍA	VALOR	DESCRIPCIÓN
CATASTRÓFICO	**5**	Riesgo cuya materialización influye gravemente en el desarrollo de procesos y el incumplimiento de los objetivos.
SEVERO	**4**	Riesgo cuya materialización dañaría significativamente el desarrollo de procesos y el incumplimiento de los objetivos.
MODERADO	**3**	Riesgo cuya materialización causaría un deterioro en el desarrollo de procesos y el incumplimiento de los objetivos.

LEVE	**2**	Riesgo que causa daño menor en el desarrollo de procesos y el incumplimiento de los objetivos.
INSIGNIFICANTE	**1**	Riesgo que puede tener un pequeño o nulo efecto en el desarrollo de proceso y que no afecta el cumplimiento de sus objetivos.

Fuente: Autores del Proyecto

Tabla 6 Escala de calificación

Calificación	**Valor**	**Riesgo**
…		
15	**3**	**Alto**
12	**3**	**Alto**
10	**3**	**Alto**
9	**2**	**Medio**
8	**2**	**Medio**
6	**2**	**Medio**
5	**2**	**Medio**
4	**1**	**Bajo**
3	**1**	**Bajo**
2	**1**	**Bajo**
1	**1**	**Bajo**

Fuente: Autores del Proyecto

5) **El resultado se presenta a través de la siguiente tabla**

Tabla 7 Matriz

Riesgo	Probabilidad	Impacto	Calificación	Evaluación del riesgo	
				Valor	Nivel
R1	2	4	8	2	Medio
R2	3	4	12	3	Alto
R3	3	4	12	3	Alto
R4	5	5	25	3	Alto
R5	1	4	4	1	Bajo
R6	2	3	6	2	Medio
R7	2	3	6	2	Medio
R8	3	3	9	2	Medio
R9	3	4	12	3	Alto
R10	1	4	4	1	Bajo
R11	1	3	3	1	Bajo
R12	4	4	16	3	Alto

Fuente: Autores del Proyecto

CONCLUSIÓN

Todos los riegos cualquiera que sea la valoración obtenida tras el análisis realizado, requieren de la estructuración de mecanismos que permitan mitigarlos y si es posible eliminarlos; sin embargo esta matriz nos permite apreciar cueles son aquellos más críticos, por lo que mediante esta información se puede estructurar un plan de contingencia estableciendo prioridades, para ello se recomienda poner en practica la guía de buenas prácticas sugerida en esta investigación.

4.3. Determinar prácticas seguras asociadas a los procesos realizados a través de la plataforma Moodle de apoyo a la presencialidad en la Unidad de Educación Virtual, para ofrecer una guía de cómo llevar los procesos de forma segura

Para la realización de este objetivo, se descargó e instaló la plataforma Moodle, en la versión 3.0.2 +, teniendo el rol de administrador, se realizaron las pruebas necesarias para verificar la seguridad de la plataforma, de esta manera se estableció una serie de tablas en las cuales se detallan las pruebas realizadas, el propósito, la descripción y una conclusión.

4.3.1. Pruebas a la plataforma Moodle

Para llevar a cabo las pruebas de seguridad de la plataforma Moodle se realizó la instalación de la última versión 3.0.2 + , la cual es la versión actuamente implementada por la Universidad.
Moodle se corrió bajo el sistema Operativo Linux UBUNTU por las siguientes razones:

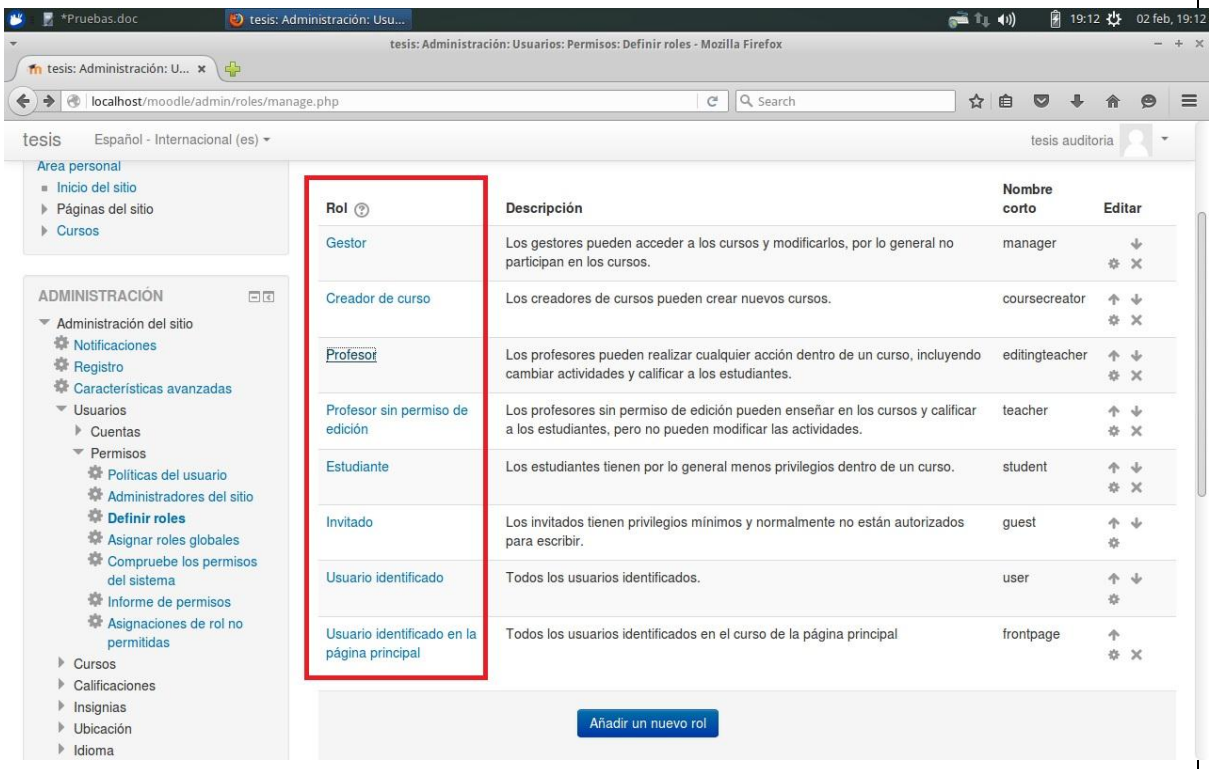
- En la universidad la plataforma Moodle está alojada en servidores cuyo sistema operativo corresponde a una versión de Linux, el propósito es hacer las pruebas bajo caracteristicas lo mas similares posibles.
- Linux es uno de los sistemas operativos más robustos , estables y rápidos.
- Linux es un sistema operativo libre.

Las pruebas realizadas se llevaron a cabo simulando ser el administrador de la plataforma de apoyo a la presencialidad, que ejerce sus labor desde la oficina de la Unidad de Educación Virtual, quien realiza la gestión de la misma, sin embargo no tiene acceso a servidores, ya que esta función se se realiza a través de la División de Sistemas de la Universidad por medio del administrador de servidores.

Tabla 8 Prueba 01

Prueba 01	Definición de roles
Propósito Determinar qué roles permite gestionar la plataforma Moodle.	
Descripción : La plataforma moodle trae por defecto 8 roles preestablecidos cada uno de ellos con ciertos privilegios y a su vez también permite añadir nuevos roles.	

Imagen 1. Definición de roles



Fuente. Autores del Proyecto

Conclusión:
La plataforma permite una gestión de roles muy completa, lo que facilita limitar los privilegios de una forma muy detallada dependiendo las necesidades.
Sin embargo se recomienda manejar la menor cantidad de roles posibles con el propósito de facilitar el seguimiento de los mismos.
Los roles que se recomienda utilizar según el análisis realizado son:

- Estudiante
- Docente
- Adminsitrador

A cada uno de ellos debe delimitarse los privilegios; solo en caso particular se puede añadir nuevos roles temporales.

Fuente. Autores del proyecto

Tabla 9 Prueba 02

Prueba 02	Asignación de privilegios

Propósito:
Determinar qué tipos de privilegios permite asignar la plataforma dependiendo de los roles previamente establecidos.

Descripción :

La plataforma Moodle permite realizar la gestión de privilegios según disponga el administrador, para ello cuenta con un listado de las acciones que se pueden habilitar o deshabilitar según se requiera, en la imagen, se muestran los privilegios asignados a el rol docente que viene prestablecido.

Imagen 2 Asignación de privilegios

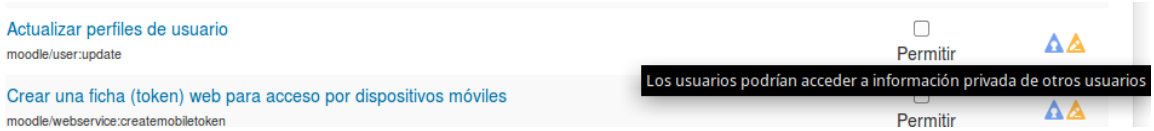
Fuente. Autores del Proyecto

Como se puede observar en la columna a la derecha se encuentra la opción **permitir** con casillas de chequeo, las cuales permiten asignar Habilitar o deshabilitar el derecho a realizar dicha acción.

De igual manera la plataforma identifica y clasifica los posibles riesgos al habilitar los

privilegios, al frente de la columna permisos se visualizan triángulos de colores con la descripción de los mismos.

Imagen 3 Roles previamente establecidos.



Fuente. Autores del Proyecto

En la imagen anterior se observa que la plataforma indica que al asignar el privilegio de actualizar los perfiles, el usuario podrá acceder a información privada de otros usuarios.

Conclusión:
Es importante realizar previamente un análisis de los privilegios antes de asignarlos y tener en cuenta las recomendaciones de posibles riesgos establecidas en la plataforma.
Se recomienda que el administrador de plataforma antes de realizar cambios en los permisos asignados a cada uno de los roles, consulte con el coordinador y que se lleve un control de los mismos mediante la documentación.

Fuente. Autores del proyecto

Tabla 10 Prueba 03

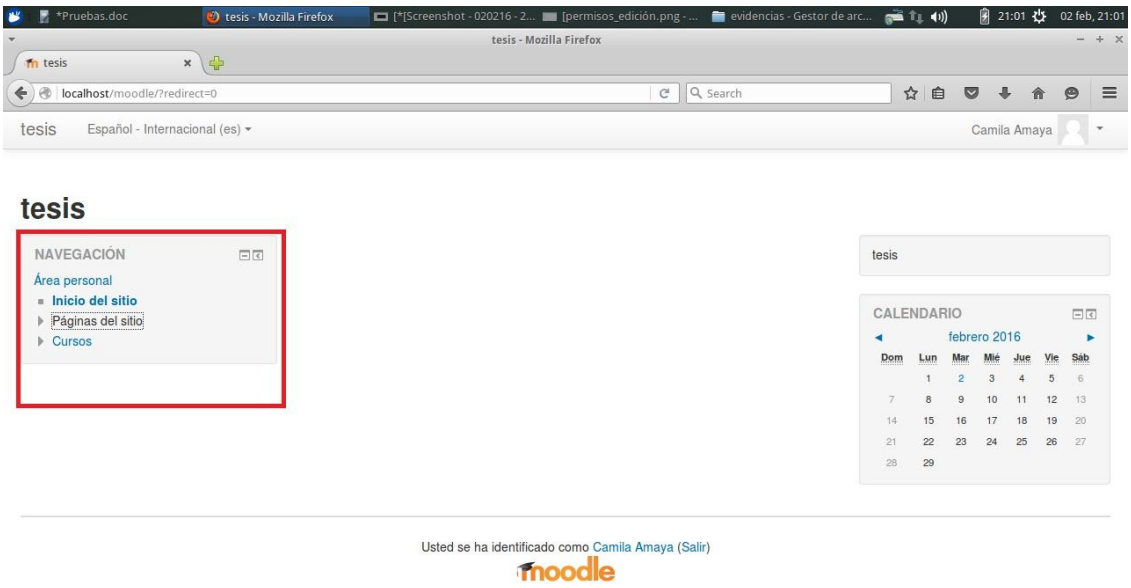
Prueba 03	Verificación de permisos asignados
Propósito: Verificar que después de asignados los privilegios, el usuario pueda acceder sólo a realizar las funciones permitidas.	
Descripción : Para la siguiente prueba se crearon usuarios nuevos y se asignaron roles de docente y estudiante, luego se verificó el menú de opciones para cada uno de los tipos de usuario mencionados. Imagen 4 Verificación de permisos asignados	

Fuente. Autores del Proyecto

En la imagen anterior se puede apreciar que existen dos usuarios estudiantes y un usuario profesor

A loguearse con el usuario **estudiante** se puede observar en la imagen a continuación, que tiene muy pocos privilegios, no tendrá acceso a cuentas de usuario, ni administrar el sitio, entre otras. Los estudiantes tienen por lo general menos privilegios dentro de un curso.

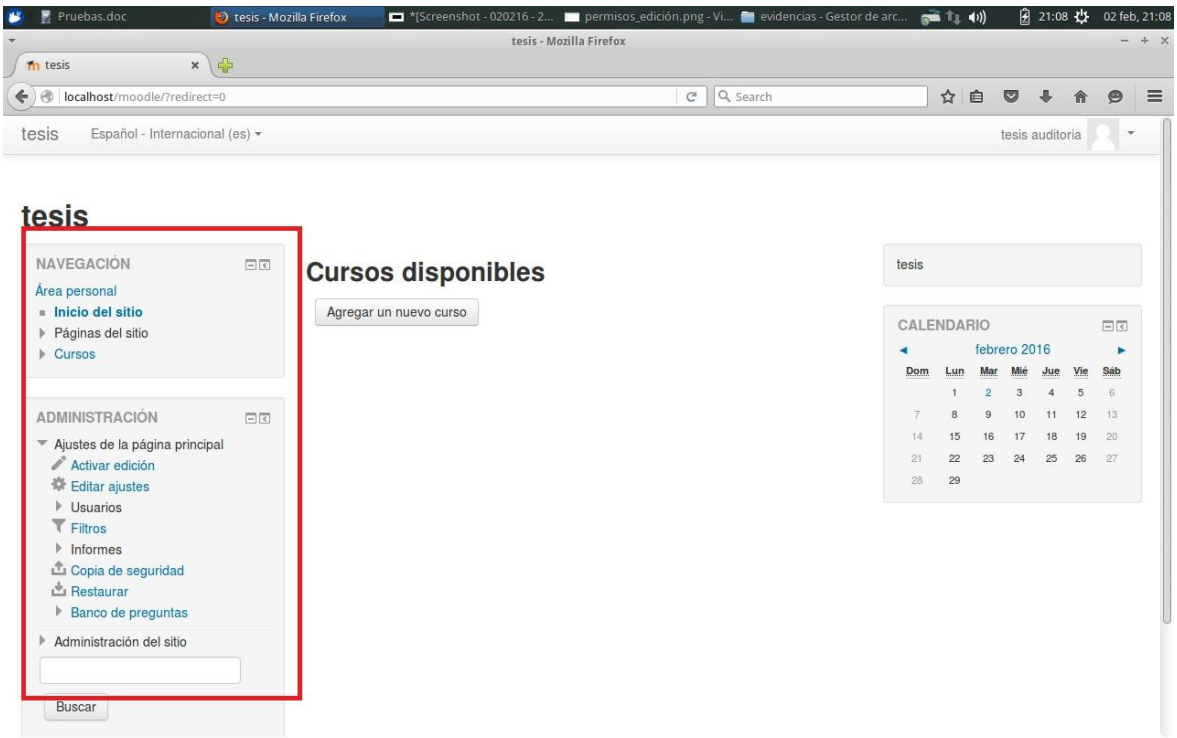
Imagen 5 Página de inicio estudiante



Fuente. Autores del Proyecto

Esta interfaz corresponde a la interfaz principal de la estudiante Camila, como se puede observar, solo posee el bloque de navegación más no el de administración.
Caso contrario ocurre con la interfaz del administrador, quien tiene asignados gran cantidad de privilegios, a continuación se muestran las opciones habilitadas para este rol de usuario administrador.

Imagen 6 Interfaz



Fuente. Autores del Proyecto

Conclusión:
Con la prueba anterior fue posible determinar que efectivamente depende de los privilegios asignados a cada rol y la asignación de los mismos, las acciones permitidas a los usuarios.
Se recomienda se tenga especial atención en la validación de permisos a asignar para cada uno de los roles, dado que por ser tantas las opciones puede ser posible la confusión.

Fuente. Autores del proyecto

Tabla 11 Prueba 04

Prueba 04	Gestión de contraseñas
Propósito: Determinar qué mecanismos de contraseña segura se aplican a través de la contraseñas en	

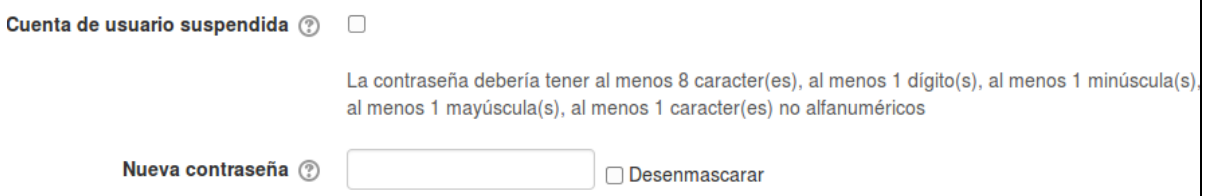
Moodle.

Descripción :

Actualmente la Universidad está implementando el proceso de unificación de contraseñas, es decir, con este proceso se pretende que los usuarios puedan acceder a cualquiera de sistemas de la institución a través de una contraseña única, dicha plataforma se rige a partir de ciertos criterios.

Desde la División de Sistemas, se genera una contraseña aleatoria a los usuarios nuevos, quienes deben ingresar con ella y posteriormente realizar el cambio de la misma respectando los criterios de contraseña segura, establecidos; en la imagen a continuación se aprecian los criterios que debieran tener las contraseñas.

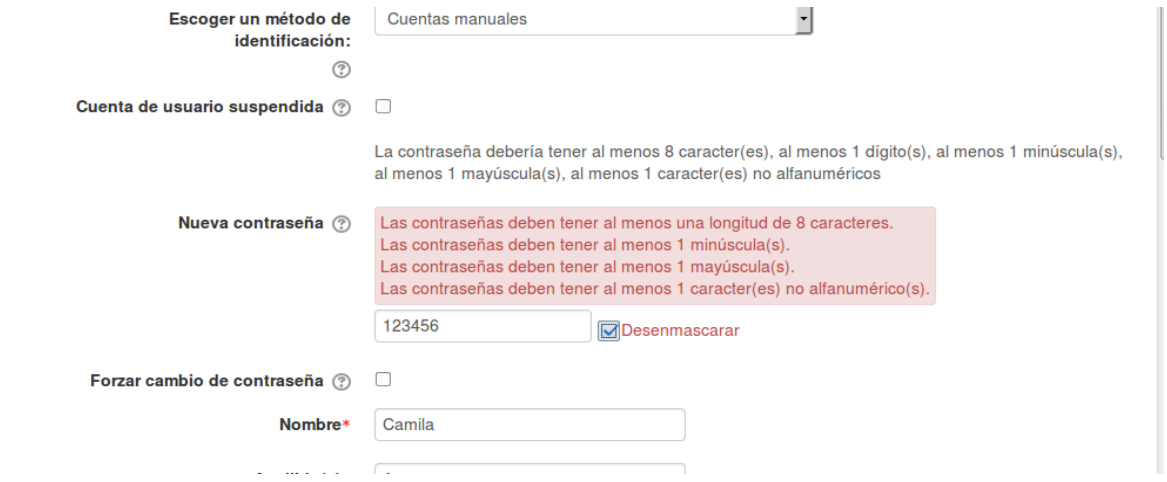
Imagen 7 Indicaciones contraseña



Fuente. Autores del Proyecto

En la siguiente imagen se muestra un error al ingresar una contraseña que no cumple los parámetros.

Imagen 8 Especificaciones contraseñas



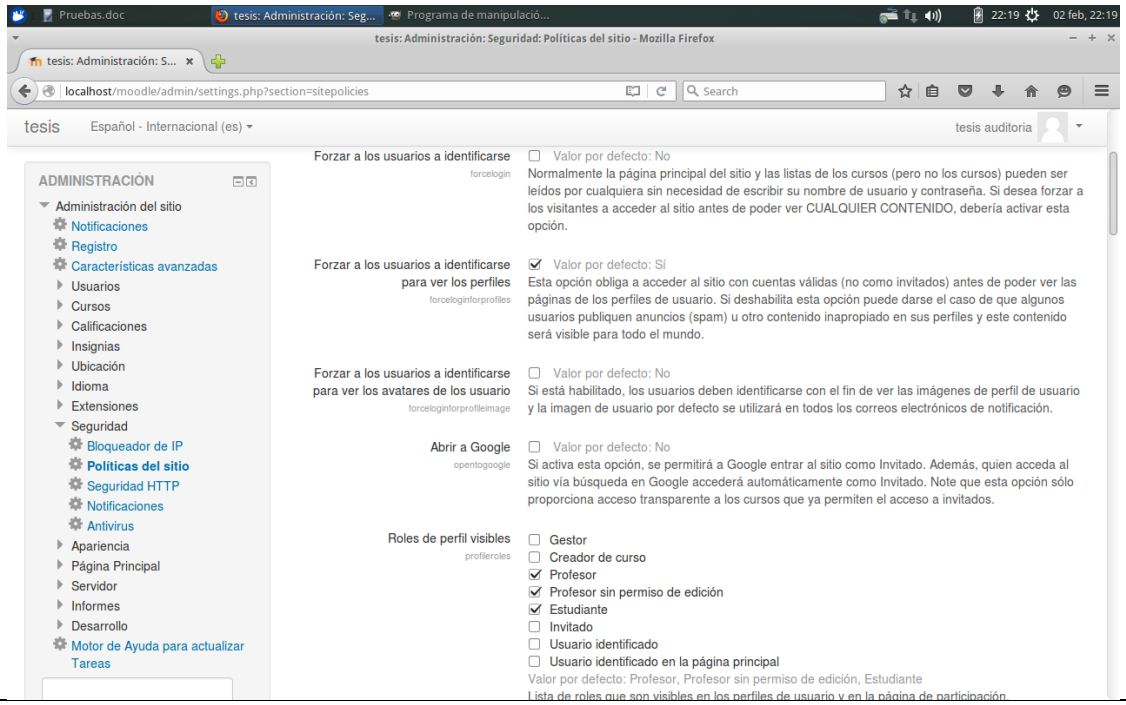
Fuente. Autores del Proyecto

Conclusión:

Con la anterior prueba, se verificó que a través de la plataforma se pueden establecer criterios de contraseña segura.

Fuente. Autores del proyecto

Tabla 12 Prueba 05

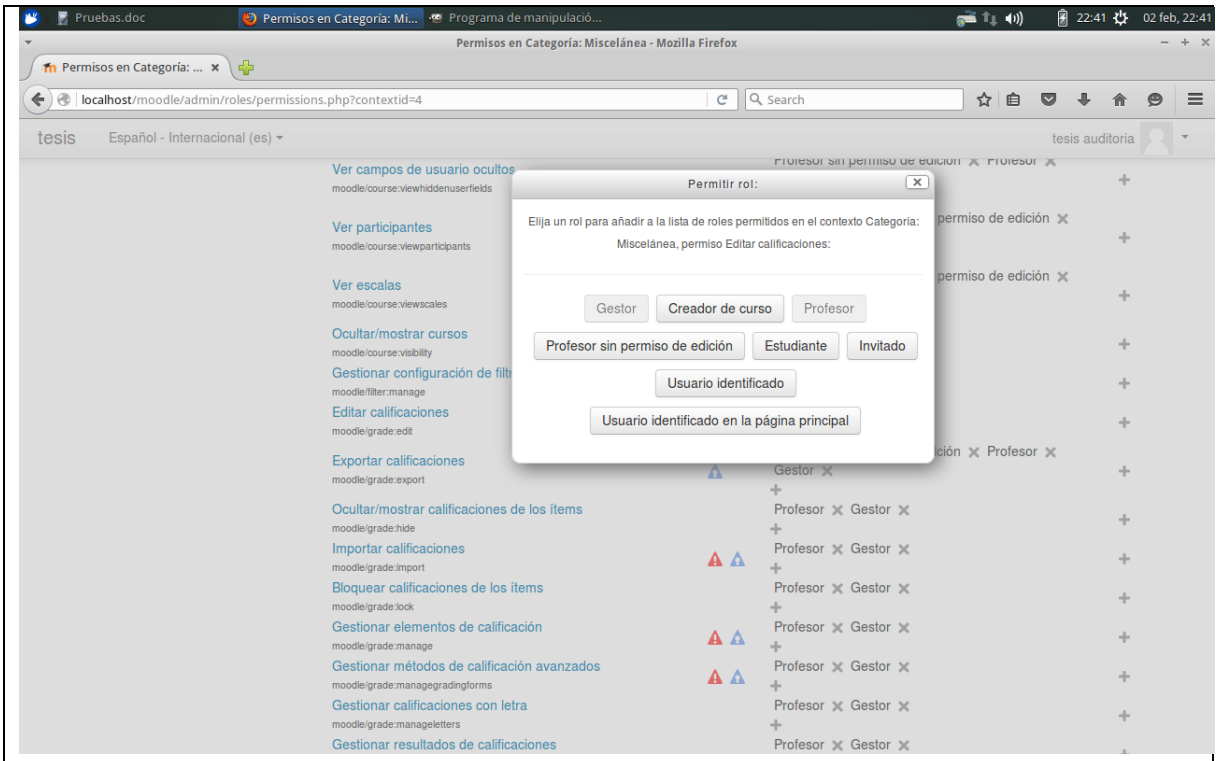
Prueba 05	Verificación de políticas del sitio
Propósito: Determinar qué mecanismos permite implementar la plataforma con el propósito restringir y controlar el acceso a la información.	
Descripción : Es importante que los usuarios cumplan ciertos requisitos de seguridad para acceder a la información manejada a través de la plataforma Moodle de apoyo a la presencialidad como: • Realizar siempre autenticación. • Cumplir con parámetros de contraseñas seguras. • Establecer tamaños máximos para la carga de archivos. • Verificación de cambios. • Tiempos de cierre de sesión. La plataforma Moodle permite la gestión de las opciones anteriormente mencionas y muchas otras, es importante regirse a través de la política de seguridad para gestionar estos parámetros. <u>Imagen 9 Verificación de políticas del sitio</u>  	

Fuente. Autores del Proyecto
Conclusión: Esta prueba permitió determinar que a través de la plataforma se pueden establecer ciertos mecanismos de seguridad que contribuyen a mantener la integridad, disponibilidad y confiablidad de la información; dado que se cuenta con la herramienta, se recomienda establecer en la política de la seguridad criterios que orienten acerca de la configuración de los mismos y su gestión.

Fuente. Autores del proyecto

Tabla 13 Prueba 06

Prueba 06	Verificación de permisos a categorías y cursos.
Propósito: Determinar qué mecanismos de seguridad se emplean para gestionar los cursos manejados a través de la plataforma Moodle de apoyo a la presencialidad.	
Descripción : Si bien es cierto que la plataforma permite la gestión de usuarios, asignación de privilegios y roles para gestionar la plataforma, también se deben aplicar controles para las categorías y cursos creados. La plataforma permite la gestión de los mismos, entre muchas estas son algunas de ellas: • Altas y bajas de usuarios • Matricular usuarios • Gestión de calificaciones • Inclusión de tareas La plataforma permite establecer cuál de los roles tiene permitidas dichas funciones, en la imagen a continuación se muestran algunos ejemplos. Imagen 10 Verificación de permisos a categorías y cursos.	



Fuente. Autores del Proyecto

Conclusión:
La plataforma permite realizar una detallada de asignación de privilegios; es importante que se definan y se documenten dichos permisos, y aplicarlos a nivel general, con el propósito de evitar que tengan que modificarse constantemente lo cual pondría en riesgo la seguridad de la información.

Fuente. Autores del proyecto

Tabla 14 Prueba 07

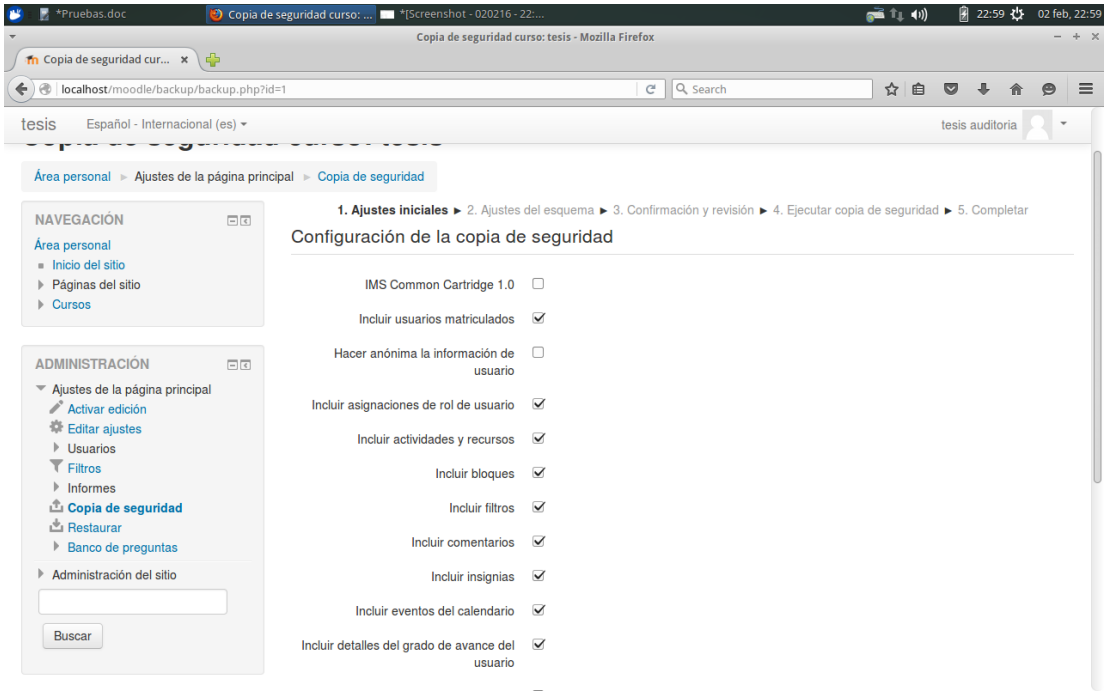
Prueba 07	Gestión de copias de seguridad
Propósito Determinar que parámetros se permiten establecer en la plataforma Moodle para generar las copias de seguridad.	
Descripción : En la plataforma es posible realizar copias de seguridad automáticas generales y específicas por cursos. Las copias de seguridad automáticas se configuran desde el servidor con cierta frecuencia de tiempo(Actualmente diarias), sobre los cursos que ha presentado actividad durante las últimas 24 horas.	

Imagen 11 Gestión de copias de seguridad

Fuente. Autores del Proyecto

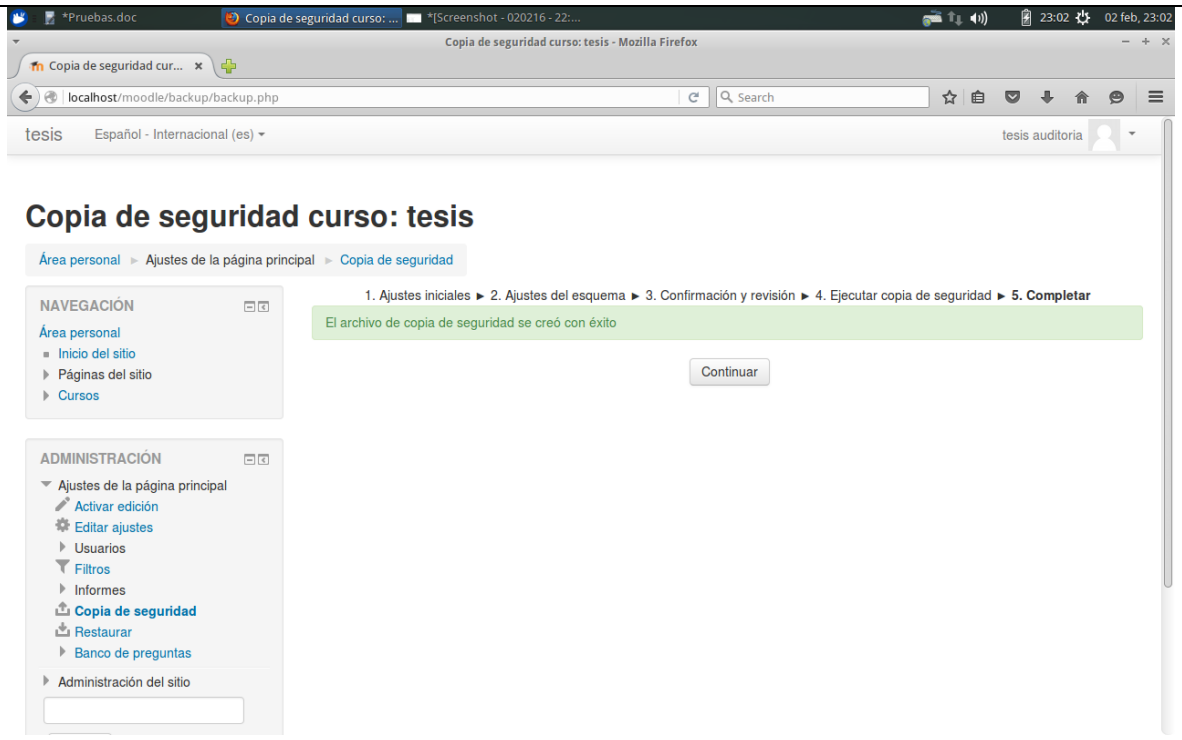
Las copias de seguridad por cursos las realiza la administradora de plataforma y las almacena en tres sitios diferentes para mayor seguridad (El equipo de cómputo o estación de trabajo, disco duro externo y en la nube (drive)).

Imagen 12 Configuración de la copia de seguridad



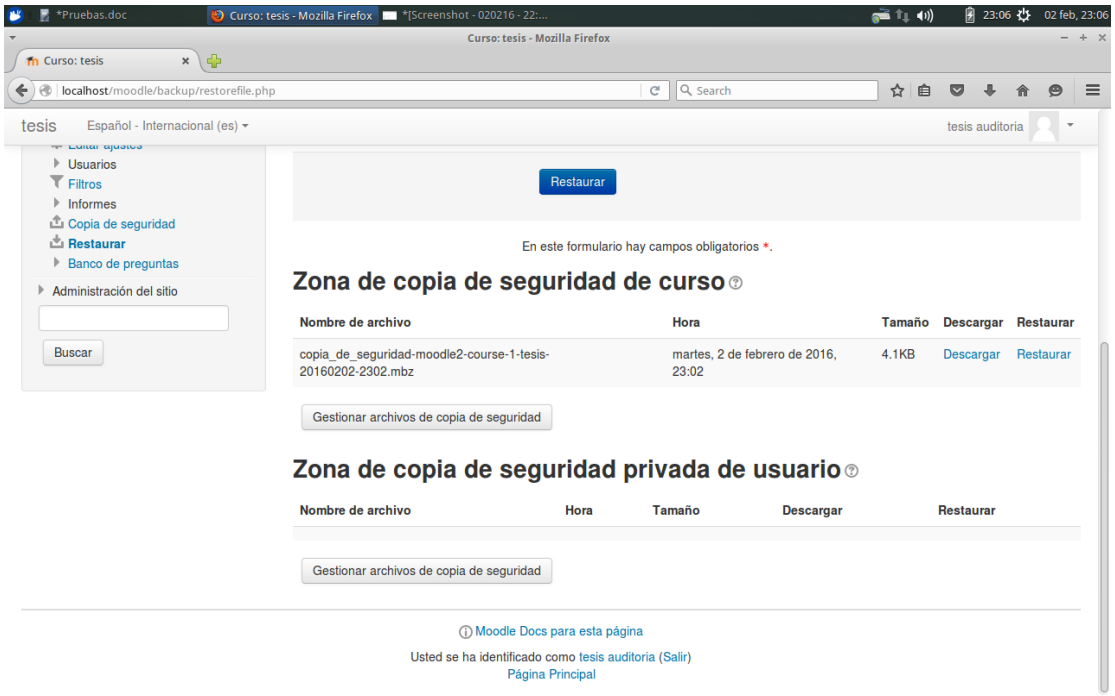
Fuente. Autores del Proyecto

Imagen 13 Completar copia de seguridad



Fuente. Autores del Proyecto

Imagen 14 Zona de copias de seguridad



Fuente. Autores del Proyecto
Conclusión: La plataforma posee todas la herramientas necesarias para la gestión de copias de seguridad, tanto para generarlas como para reestaurarlas. Es necesario llevar un registro de las copias de seguridad que se realizan. De igual manera se recomienda que cada vez que se vaya a realizar un cambio significativo en la plataforma, se active el **modo mantenimiento** para evitar inconvenietes a los usuarios y cualquier riesgo a la integridad de la información.

Fuente. Autores del proyecto

4.4. Estructurar el documento de buenas prácticas que oriente en la gestión de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialdiad en la Unidad de Educación Virtual, para establecer el propósito, recomendaciones y actividades, necesarios de la gestión segura de la información.

Para el cumplimiento de este objetivo específico, se revisó y verificó la información recolectada en las pruebas anteriores y se estableció unas tablas para la estructuración de la guía, en la cual, se detalla, el dominio, el objetivo de control y el control, y para cada uno de ellos, se describió el propósito, unas recomendaciones y actividades.

4.4.1. Guía de buenas prácticas

En la Universidad Francisco de Paula Santander Ocaña (UFPSO), al igual que en la mayoría de las empresas, la información es considerado como el activo más importante, como tal es necesario aplicar controles y/o estrategias que permitan realizar el debido seguimiento a la misma, con el propósito de mantener la integridad, confidencialidad y disponibilidad.

Los riesgo y las amenazas siempre van a existir, por lo que las empresas deben buscar las estrategias que les permitan analizar esos riesgos, determinar su frecuencia y su impacto para así, de esta manera establecer las posibles soluciones que permitan minimizarlos y si es posible y viable eliminarlos por completo.

Para el caso específico de la Unidad de Educación Virtual de la UFPSO donde se maneja la plataforma Moodle como apoyo a la prespecialidad, estas tres características de la información ya mencionadas (disponibilidad, confidencialidad e integridad) son esenciales para brindar un servicio de calidad; esta plataforma es implementada por los docentes del Alma Mater para mejorar su metodología presencial, mediante ella ofrecen a los estudiantes la oportunidad de adquirir nuevos conocimientos para su formación profesional de la mano con la tecnología.

Sin duda la Unidad de Educación Virtual requiere la construcción y puesta en práctica de una guía de buenas prácticas, las cuales al ser implementadas permitan una gestión

competente y efectiva de la seguridad de la información maneja a través de la plataforma de apoyo a la prespecialidad.

Para la creación de dicha guía nos apoyaremos en la norma ISO 27002 del 2013 en la cual mediante los objetivos de control planteados describe los aspectos a analizar para garantizar la seguridad de la información.

Esta guía no pretende ser de obligatorio cumplimiento, sino de carácter informativo, mediante ella se proporcionará una orientación a los procesos basados en la norma en mención, de manera que con la aplicación voluntaria de la misma sea posible mantener la disponibilidad, confidencialidad e integridad del activo más importante "La información".

Objetivo: Estructurar el documento guía buenas prácticas que oriente en la gestión segura de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialdiad en la Unidad de Educación Virtual.

Alcance: El trabajo se presenta como una guía de buenas prácticas para la Seguridad de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialidad implementada en la Universidad Francisco de Paula Santander Ocaña y administrada desde la Unidad de Educación Virtual de la Institución, con esta se pretende formular una serie de orientaciones en la aplicación de controles. Las actividades formuladas no serán desarrolladas, solo se presentarán como una parte necesaria de los controles.

<table>
<tr><td>Dominio</td><td>5</td><td colspan="3">Políticas de Seguridad</td></tr>
<tr><td>Objetivo de Control</td><td rowspan="2">Directrices de la Dirección en seguridad de la información.</td><td>Control</td><td rowspan="2">Conjunto de políticas para la seguridad de la información</td></tr>
<tr><td>5.1</td><td>5.1.1</td></tr>
<tr><td colspan="4">DESARROLLO</td></tr>
<tr><td colspan="4">Propósito

Instaurar la política de seguridad que permita formalizar el compromiso con la gestión segura de la información manejada en la Unidad de Educación Virtual de Universidad Francisco de Paula Santander Ocaña (UFPSO), para que a través de esta, se puedan orientar los procesos y mantener tres de las características más importantes de la información que son la disponibilidad, integridad y confidencialidad.</td></tr>
<tr><td colspan="4">Recomendación

La implementación de la política de seguridad de la información requiere un gran sentido de pertenencia en la que los directivos y el comité de la seguridad se comprometan para que se cumpla el objetivo de la misma.</td></tr>
</table>

La UFPSO cuenta actualmente con una política de seguridad, sin embargo la misma se plantea a manera general para todo la institución, se recomienda que se formalice una política específica para la Unidad de Educación Virtual en la se especifiquen los requerimientos propios en pro de alcanzar los objetivos.

Actividades

a) Delegar a un grupo de personas la responsabilidad de la seguridad de la información, mediante la conformación de un comité de seguridad.

El comité de gestión de la seguridad de la información debe:

- Evaluar los procesos.
- Revisar la efectividad de la política.
- Determinar cambios significativos.
- Determinar mecanismos mejoren las falencias detectadas.
- Aprobar o desaprobar la asignación de responsabilidades en cuanto a la seguridad de la información.
- Asegurar que se implementen los controles
- Evaluar con frecuencia la política de seguridad de la información.
- Comunicar a los directivos las decisiones tomadas.

Dominio	**5**	**Políticas de Seguridad**		
Objetivo de Control		Directrices de la Dirección en seguridad de la información.	**Control**	Revisión de las políticas para la seguridad de la información.
5.1			**5.1.2**	

DESARROLLO

Propósito

La política de seguridad de la información es una herramienta esencial para mantener la integridad, confidencialidad y disponibilidad de la información, sin embargo, para que la finalidad del mismo se cumpla, dicha política debe ser revisada constantemente en búsqueda de oportunidades de mejoramiento, de ser necesario, actualizarla y finalmente las modificaciones deben ser conocidas por el personal a cargo.

Recomendación

- El personal encargado de la seguridad de la información debe cerciorarse de los tiempos establecidos para la revisión de la política se cumplan y que se lleve un control de las modificaciones realizadas a la misma.

Actividades

a) Establecer una frecuencia de tiempo para revisión de la política dentro del comité de seguridad de la información.
b) Analizar la certeza de la política y detectar necesidades mediante mecanismos que les permitan evaluar la efectividad de la misma.
c) Dejar por escrito las actualizaciones y/o modificaciones realizadas a la misma.
d) Realizar reuniones semestrales para dar conocer al personal directamente relacionado, las novedades a cerca de la política y concientizar acerca de la importancia de la seguridad de la información.
e) Establecer dentro del contrato una cláusula que especifique la obligatoriedad de la aplicación de la política en el ejercicio de su cargo si fuese necesario.

Dominio	**6**	Aspectos organizativos de la seguridad de la información		
Objetivo de Control		Organización interna.	**Control**	Asignación de responsabilidades para la seguridad de la información.
6.1			**6.1.1**	

DESARROLLO

Propósito

Asignar y comunicar responsabilidades tanto generales como particulares donde se den a conocer las expectativas de los directivos en cuanto a la seguridad de la información, dichas responsabilidades implican compromiso en realizar las acciones necesarias que permitan proteger la información que se encuentre bajo su custodia.

Recomendación

Es importante tener claridad de cada uno de los procesos que se realizan en la gestión de la plataforma Moodle de apoyo a la presencialidad y asignar al personal con el perfil adecuado la responsabilidad de los mismos de tal forma que estén en la capacidad de contribuir con la protección de este importante activo (La información).

Actividades

a) Identificar claramente los procesos.
b) Determinar con qué perfil debe contar el personal para asumir la responsabilidad de uno a varios procesos.
c) Documentar detalladamente las responsabilidades asignadas y la persona a cargo de las mismas.
d) Evaluar frecuentemente la eficacia de las acciones realizadas por el personal para cumplir son sus responsabilidades.
e) Establecer y dar a conocer al personal las penalidades que podrían ser asignadas en caso de que no cumplan con sus responsabilidades le ocasione poner en riesgo la seguridad de la información.

Dominio	**6**	Aspectos organizativos de la seguridad de la información		
Objetivo de Control		Organización interna.	**Control**	Segregación de tareas
6.1			**6.1.2**	

DESARROLLO

Propósito

Realizar una distribución adecuada de las tareas o funciones de manera que cada una de ellas pase por los procesos básicos que son la aprobación, ejecución, evaluación y documentación, esto conlleva a evitar errores involuntarios o acciones inapropiadas que alguna persona predispuesta pueda cometer y que atenten contra la seguridad de la información.

Recomendación

Es importante que los procesos realizados no sean realizados y evaluados por la misma persona dado que en muchas ocasiones a uno mismo no le es posible identificar errores por lo que la segregación de tareas representa una actividad de control clave para la efectividad de los procesos.

Actividades

a) Evaluar el recurso de personal existente y el perfil de cada uno de ellos.
b) Establecer adecuadamente el flujo de trabajo.
c) Designar tareas de forma equitativa de forma que las funciones de aprobación, ejecución y evaluación en lo posible no sean desarrolladas por la misma persona.

Dominio	**6**	Aspectos organizativos de la seguridad de la información		
Objetivo de Control		Organización interna.	**Control**	Contacto con las autoridades.
6.1			**6.1.3**	

DESARROLLO

Propósito

Establecer y mantener un listado de relaciones necesarias con autoridades que puedan intervenir y establecer las medidas necesarias en asuntos de seguridad.

Recomendación

Es de significativa importancia que la Unidad de Educación Virtual conozca y documente a que autoridad debe acudir en caso de presentarse irregularidades ya sean voluntarias e involuntarias que atenten contra la integridad, confidencialidad y/o

disponibilidad de la información que se maneja a través de la plataforma Moodle de apoyo a la presencialidad, estas autoridades son las encargadas de establecer las penalidades (de ser necesarias) o acciones a seguir en cualquiera de los casos que se presenten.

Actividades

a) Determinar el conducto regular a seguir en la dependencia Unidad de Educación Virtual.
   Primea instancia: **Coordinador de la Unidad de Educación Virtual** (Jefe inmediato).
   Segunda instancia: Jefe de dependencia involucrada.
   Tercera instancia: Dado que la Unidad de Educción Virtual es una dependencia adscrita a la subdirección académica, la siguiente autoridad a cargo es el **Subdirector Académico.**
   Última instancia: La Máxima autoridad en la institución, **El Director**.

b) Documentar el listado de autoridades.
c) Revisar frecuentemente y actualizar de ser necesario.
d) Llevar un registro de las modificaciones realizadas.

Dominio	**6**	Aspectos organizativos de la seguridad de la información		
Objetivo de Control		Organización interna.	**Control**	Contacto con grupos de interés especial.
6.1			**6.1.4**	

DESARROLLO

Propósito

Mantener líneas de comunicación apropiada y efectiva con los grupos de interés especial como la policía, la defensa civil y bomberos para que puedan ser contactados fácilmente y de forma oportuna en caso de que se presente algún incidente de seguridad de la información que no pueda resolverse internamente.

Recomendación

- La Unidad de Educación Virtual debe tomar todas las medidas de seguridad posibles, aunque algunas de ellas parezcan poco probables no se debe desistir de estas.
- Los incidentes de seguridad se presentan en diferentes circunstancias, algunas se resuelven internamente en la institución y otras requieren de grupos de interés especial como es el caso de la defensa Civil, la Policía Nacional y los bomberos.

- Es importante que la Unidad Virtual mantenga dichas relaciones de la mejor manera.

Actividades

a) Un representante de la Unidad de Educación Virtual debe visitar las instalaciones de los grupos de interés especial (Policía Nacional, la defensa civil, los bomberos y otros que considere necesarios) y solicitar su atención oportuna en casos particulares en los que se requiera su presencia.
b) Mantener por escrito los principales datos de los grupos de interés social.
c) Verificar con determinada frecuencia que los datos estén vigentes, de lo contrario realizar las actualizaciones correspondientes.

Dominio	**6**	Aspectos organizativos de la seguridad de la información		
Objetivo de Control		Organización interna.	**Control**	Seguridad de la información en la gestión de proyectos.
6.1			**6.1.5**	

DESARROLLO

Propósito

Contemplar la seguridad de la información en la gestión de proyectos.

Recomendación

Independientemente del proyecto que va ser desarrollado o puesto en marcha, el líder del equipo debe buscar estrategias que le permitan brindar seguridad la información que se maneja a través de ellos y llegar a un feliz término los mismos.

Actividades

- Planear y definir objetivos del proyecto
- Identificar el grado de seguridad requerido dependiendo de la información a manejar
- Liderar un equipo de trabajo y asignar responsabilidades
- Asegurarse de que los recursos necesarios para el proyecto se encuentren disponibles.
- Monitorear y documentar cada una de las fases del proyecto.

Dominio	**6**	Aspectos organizativos de la seguridad de la información		
Objetivo de Control		Dispositivos para movilidad y teletrabajo.	**Control**	Política de uso de dispositivos para movilidad

6.2		6.2.1	

DESARROLLO

Propósito

Establecer una política y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil.

Recomendación

Cuando se utilizan dispositivos informáticos móviles y computadores portátiles pesados, tarjetas inteligentes y teléfonos móviles se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura de la institución.
La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto.
Se deberían desarrollar normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención acerca de portar un equipo valioso.
- No poner identificaciones de la institución en el dispositivo, salvo los estrictamente necesarios.
- No poner datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada.

Actividades

- Se debiera establecer procedimientos para estos dispositivos, que abarquen los siguientes aspectos:
- La protección física necesaria
- El acceso seguro a los dispositivos
- La utilización segura de los dispositivos en lugares públicos.
- El acceso a los sistemas de información y servicios de la institución a través de dichos dispositivos.
- Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
- Los mecanismos de resguardo de la información contenida en los dispositivos.
- La protección contra software malicioso.
- Entrenar al personal que los utiliza o utilizará.

Dominio	**7**	Seguridad ligada a los recursos humanos		
Objetivo de Control		Antes de la contratación.	Control	Investigación de antecedentes.

7.1		**7.1.1**	

DESARROLLO

Propósito

Establecer los controles necesarios para verificar los antecedentes del personal a vincular a la dependencia, esto en concordancia con las leyes, regulaciones y ética relevantes.

Recomendación

Cuando se requiera la contratación de personal ya sea para un puesto nuevo o para ascenso se deberá realizar la respectiva investigación de antecedentes judiciales, disciplinarios y personales a fin de contratar personas idóneas para el cargo.

Actividades

- En caso de halla necesidad de contratar personal para la Unidad de educación virtual, más específicamente personal que deba tener acceso a la información que se maneja a través de la plataforma Moodle de apoyo a la presencialidad se deberá realizar un chequeo minucioso de antecedentes que incluya:

  a) Disponibilidad de referencias de carácter personal y laboral
  b) Chequeo completo de la hoja de vida (currículum vital – CV) del postulante en cuanto integridad y exactitud.
  c) Verificación de legitimidad de títulos académicos y profesionales.
  d) Comprobación de su identidad.
  e) Certificados de antecedentes personales, disciplinarios y judiciales.

Dominio	**7**	Seguridad ligada a los recursos humanos	
Objetivo de Control	Antes de la contratación.	Control	Términos y condiciones de contratación.
7.1		**7.1.2**	

DESARROLLO

Propósito

Definir las funciones y responsabilidades para cada uno de los puestos de trabajo de la dependencia que involucren el manejo y/o acceso a la plataforma Moodle de apoyo a la presencialidad, para lo que es necesario establecer los privilegios imperiosos para el desarrollo de la labor.

Recomendación

El personal a contratar debe conocer sus funciones y responsabilidades por lo que es deber de la autoridad encargada realizar formalmente la comunicación clara y precisa de las mismas, dado que se tendrá acceso a la información manejada a través de la plataforma para el desarrollo de su labor, es imprescindible que también conozcan la importancia y la obligación que adquiere con la institución una vez contratado y aun después de finalizar su trabajo, de no divulgar por ningún motivo la información confidencial por lo que es importante que se instituya un acuerdo de confidencialidad.

Los contratos establecidos por la Universidad contienen una cláusula de confidencialidad sin embargo este no es específico para cada uno de los puestos y en muchas ocasiones es pasada por alto, por lo que se propone que se establezca un documentos específico (Acuerdo de confidencialidad entre el administrador de la plataforma y la Universidad) en el que se detallen las obligaciones de no divulgación, y las consecuencias en caso de no acatarlo.

Actividades

- La coordinadora de la Unidad de Educación Virtual debe:
  a) Dar a conocer claramente las funciones y responsabilidades correspondientes, las cuales se encuentran estipuladas en la estructura orgánica de la dependencia.
  b) Recalcar la importancia de mantener la integridad, disponibilidad y CONFIDENCIALIDAD de la información que se maneja a través de la plataforma.
  c) Dar a conocer el acuerdo de confidencialidad y posterior firma.

Dominio	**7**	Seguridad ligada a los recursos humanos	
Objetivo de Control	Durante la contratación.	Control	Responsabilidades de gestión.
7.2		**7.2.1**	

DESARROLLO

Propósito

Determinar la importancia en el liderazgo en la gestión de responsabilidades y compromisos designados al personal contratado.

Recomendación

El coordinador de la Unidad de Educación virtual se convierte en la base de la organización y de la gestión de cada uno de las labores a desarrollar en la dependencia, es este quien debe llevar a cabo los mecanismos necesarios para dar seguimiento al trabajo desarrollado y la mejora de los mismos con el paso del tiempo y las experiencias adquiridas.

Actividades

- Establecer responsabilidades, obligaciones y derechos de las personas.
- Desplegar la estrategia y la visión a todos los niveles y personas.
- Formalizar y mejorar un modelo organizativo que defina las interrelaciones y las herramientas de gestión de las diferentes actividades y procesos de la gestión de la plataforma Moodle de apoyo a la presencialidad.

Dominio	**7**	Seguridad ligada a los recursos humanos		
Objetivo de Control		Durante la contratación.	Control	Concienciación, educación y capacitación en seguridad de la información.
7.2			**7.2.2**	

DESARROLLO

Propósito

Capacitar al personal de la Unidad de Educación Virtual a cerca de las políticas y procedimientos institucionales de acuerdo a las funciones y responsabilidades que tenga a cargo.

Recomendación

Al ser contratado al personal se le concientiza de la importancia de la seguridad de la información que se maneja en la dependencia, sin embargo no debe quedarse allí es importante que se capacite constantemente sobre la importancia de la seguridad del tratamiento adecuado de los datos, lo que incluye las actualizaciones a las políticas de seguridad y los planes de contingencia, esto contribuye en gran medida a que se disminuyan los errores y se realice un buen desempeño de las funciones y responsabilidades asignadas.
Del mismo modo es importante que se capacite constantemente al personal sobre las actualizaciones de la plataforma Moodle y sobre el manejo adecuado de todas las nuevas herramientas que cuenta dicha actualización, esto garantiza la mejora del servicio.

Actividades

- Programar capacitaciones frecuentes a todo el personal en general sobre la seguridad de la información y del uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad.
- Concientizar sobre las sanciones a ser aplicadas por incumplimiento de las Políticas en seguridad y en el tratamiento de incidentes de seguridad que requieran de su intervención.
- Programar semestralmente capacitaciones al personal encargado de administrar la plataforma Moodle sobre las herramientas que ofrece la plataforma.

Dominio	**7**	Seguridad ligada a los recursos humanos

Objetivo de Control	Durante la contratación.	Control	Proceso disciplinario.
7.2		**7.2.3**	

DESARROLLO

Propósito

Garantizar el buen desempeño del personal de la Unidad de Educación Virtual, que cumplan con sus deberes sin incurrir en prohibiciones, establecer los procesos disciplinarios y las sanciones a las que serían sometidos en caso de incumplir sus responsabilidades mediante la implantación de un proceso disciplinario.

Recomendación

La Unidad Virtual de acuerdo a lo que dicta la ley debe documentar las acciones que puedan incurrir en sanciones disciplinarias y cual es procedimientos que se debe llevar a cabo para cada uno de dichos casos.

Actividades

- Dar a conocer en profundidad al personal el modelo disciplinario y su operación.
- Establecer dentro del contrato una cláusula de obligatoriedad de dar cumplimiento a la política de seguridad de la información.

Dominio	**7**	Seguridad ligada a los recursos humanos	
Objetivo de Control	Cese o cambio de puesto de trabajo.	Control	Cese o cambio de puesto de trabajo.
7.3		**7.3.1**	

DESARROLLO

Propósito

Establecer el procedimiento a seguir en caso de presentarse desvinculación del puesto de trabajo o cambio de funciones.

Recomendación

En pro de mantener la seguridad de la información es imprescindible que se den a conocer las responsabilidades de terminación de funciones, lo que incluye la confidencialidad de la información a la que tuvo acceso durante el desarrollo de sus funciones.

Actividades

- Retirar los privilegios de acceso a la información que ya no hace parte de sus funciones ya sea porque cambia de puesto o porque se desvincula por completo de la dependencia.

- Recordar al funcionario los procedimientos instaurados en el acuerdo de confidencialidad.

Dominio	**8**	Gestión de activos		
Objetivo de Control		Responsabilidad sobre los activos.	Control	Inventario de activos
8.1			**8.1.1**	

DESARROLLO

Propósito

Identificar los principales activos de información en la Unidad de Educación Virtual, los cuales deben estar claramente identificados.
Nota: Entiéndase por activo todo aquel elemento que represente valora para la dependencia, no solo los activos físicos sino también los activos de información.

Recomendación

En la dependencia debe existir debidamente documentado un inventario de activos en que se identifiquen uno a uno y que se clasifiquen por su tipo todos los elementos que presenten valor para la dependencia.

Actividades

- Documentar todos los activos de información con los que se cuente en la plataforma Moodle de apoyo a la presencialidad.
- Mantener actualizado el inventario de activos.

Dominio	**8**	Gestión de activos		
Objetivo de Control		Responsabilidad de los activos	**Control**	Propiedad de los activos
8.1			**8.1.2**	

DESARROLLO

Propósito
Lograr mantener la protección adecuada de los activos de la organización identificando los dueños para todos los activos.
Asignar la responsabilidad para el mantenimiento de los controles adecuados.

Recomendación

Se debiera asegurar que los activos de información sean debidamente clasificados considerando su criticidad, definiendo y revisando periódicamente los accesos de acuerdo a la política correspondiente.

Actividades

- Asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente en función a su valor.
- Definir y revisar periódicamente los requisitos de seguridad y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.
- Velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

Dominio	**8**	Gestión de activos		
Objetivo de Control		Responsabilidad sobre los activos.	Control	Uso aceptable de activos
8.1			**8.1.3**	

DESARROLLO

Propósito

Identificar, documentar e implantar regulaciones para el uso adecuado de la información y demás los activos.

Recomendación

En la gestión de la plataforma Moodle de apoyo a la presencialidad, el activo más importante es la información que se maneja a través de ella como es el caso de datos de usuario, notas, contenidos de cursos entre otros, por lo que se realiza la asignación de responsabilidades al personal con el perfil idónea para manejo seguro de la misma, por lo que estos no deben realizar ningún proceso al que no esté autorizado.

Es necesario definir un documento en el que se especifiquen las responsabilidades del personal con los activos asignados bajo su responsabilidad en el que se consideren como mínimo los siguientes ítems:

- Por ningún motivo se debe divulgar información confidencial de la dependencia, durante o después del desarrollo de sus labores como persona de la Unidad Virtual.
- Los privilegios asignados para el manejo de la plataforma se limitan específicamente a los necesarios para el desarrollo de la labor y responsabilidad

establecida para cada empleado.

- Está prohibida la divulgación de contraseñas.
- No se debe establecer conexiones a redes externas.
- Cerrar todas las cesiones al finalizar la jornada laboral.
- No se debe alterar de ninguna formar el hardware o software sin ser autorizado.
- No migrar a una nueva versión de Moodle sin previa autorización y sin antes haber realizado las copias de seguridad necesarias para garantizar el servicio.
- Respetar los derechos de autor.
- No utilizar de ninguna manera la plataforma para uso personal.
- Informar de todo acto sospechoso detectado o incidente.

Actividades

- Estructurar un documento de políticas para el uso aceptable de los activos.
- Realizar revisiones y actualizaciones constantes del mismo.
- Establecer dentro del contrato una cláusula en al que se indique la obligatoriedad de cumplir con las políticas establecidas por la dependencia.
- Capacitar al personal acerca de dicha política y concientizar sobre la importancia de la misma.

Dominio	**8**	Gestión de activos		
Objetivo de Control		Responsabilidad sobre los activos.	Control	Devolución de activos
8.1			**8.1.4**	

DESARROLLO

Propósito

Establece las formalidades necesarias a seguir, para garantizar la adecuada protección y devolución de los activos de la Unidad de Educación Virtual una vez finalizado el contrato o las actividades relacionadas al uso de los mismos.

Recomendación

Una vez finalizado el contrato, o que se debe realizar cambió de un sitio de trabajo o que se haya terminado el tiempo autorizado para hacer uso de algún activo, es deber del empleado realizar la entrega del mismo, de igual manera es deber del coordinador o el encargado realizar formalmente y en óptimas condiciones los activos y elaborar un informe del estado de los mismos.

Se debe aclarar que los activos en mención no se refieren solamente a físicos sino también a archivos digitales.

Actividades

- Redactar un formato de solicitud de devolución que contenga como mínimo los siguientes campos:

a) Nombre de quien realiza la devolución
b) Nombre de quien recibe lo devuelto
c) Fecha
d) Motivo de la devolución
e) Activos a devolver son su respectivo análisis.

- Se debe verificar que activos tenía a disposición el usuario que realiza la devolución.
- En caso de ser activos digitales, las contraseñas de acceso deben ser modificadas o los privilegios removidos.

Dominio	**8**	Gestión de activos		
Objetivo de Control		Clasificación de la información	Control	Directrices de clasificación
8.2			**8.2.1**	

DESARROLLO

Propósito

Definir directrices para la clasificación de la información según el nivel de protección que requiera, requisitos legales, sensibilidad y criticidad para la Organización.

Recomendación

Este proceso de clasificación resulta ser tedioso si desde el principio no se ha realizado cierta clasificación, se deben establecer categorías generales para posteriormente distribuir la información en cada una de ellas.

En la Unidad de Educación virtual se cuenta con información física archivada por carpetas, esto ayudará a que el proceso de clasificación de las mismas sea más sencillo.

Actividades

a) Establecer Categorías generales tanto para archivos digitales como físicos como:
   - Documentos legales.
   - Documentación interna.
   - Formatos
   - Gestión de la plataforma Moodle de apoyo a la presencialidad

- Informes
- Acceso publico
- Entre otras que se consideren necesarias

b) Distribuir los documentos según las categorías creadas.
c) Definir para cada una de esas categorías el grado de seguridad que requieren.
d) Establecer mecanismos de gestión.
e) Establecer normas de acceso a la información contenida en cada una de las categorías.

Dominio	**8**	Gestión de activos		
Objetivo de Control		Clasificación de la información	Control	Etiquetado y manipulado de información
8.2			**8.2.2**	

DESARROLLO

Propósito

Implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información de acuerdo al esquema adoptado por la Unidad de Educación Virtual

Recomendación

El etiquetado facilita la manipulación de archivos y la aplicación de mecanismos para mantener su integridad, disponibilidad y confiablidad, se debe establecer pautas con las que se realice el procedimiento de etiquetado y documentarlo para una fácil comprensión del mismo.

Actividades

- Crear tablas de redacción documental, establecer niveles de jerarquía, desglosar de allí la demás información utilizando nomenclatura de acuerdo al tipo de información.

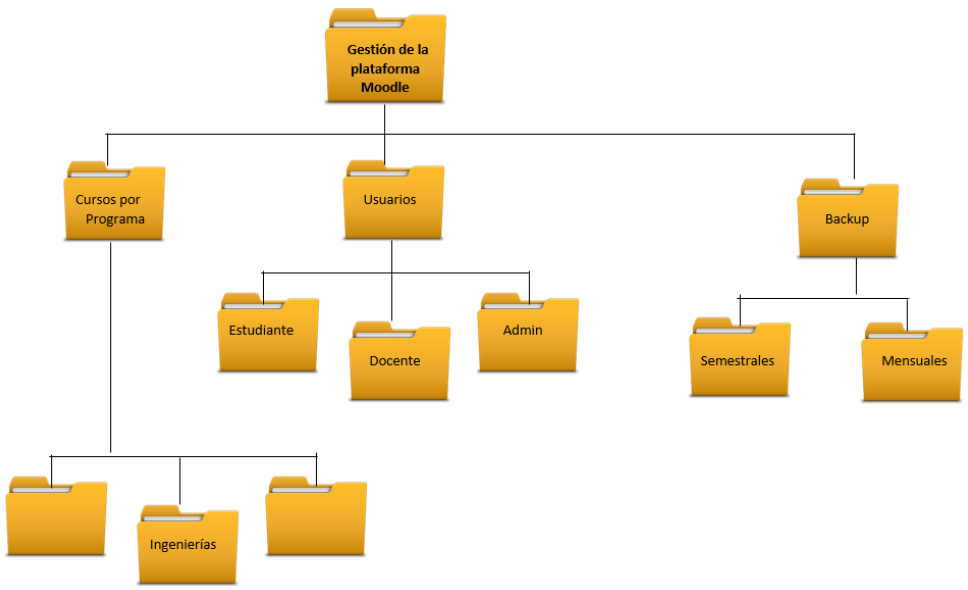
- Para un formato de registro de usuarios de la plataforma Moodle de apoyo a la presencialidad.

- En caso de información física se pude realizar la misma distribución jerárquica y utilizar rótulos para identificarlos.

- Realizar la respectiva documentación y frecuente actualización.

Así por ejemplo

1. GPM_Documentación
1.1 GPM_Cursos
1.1.1 GPM_Cursos_Ingeniería
1.1.2 GPLM_Cursos_Admnistración
1.2 GPM_Usuarios
1.2.1 GPM_Usuarios_Estudiante
1.2.2 GPM_Usuarios_Docente
1.2.3 GPM_Usuarios_Administrativo
1.3 GPM_Backup
1.3.1 GPM_Backup_semestrales
1.3.1 GPM_Backup_Mensuales
…..
…..



Dominio	**8**	Gestión de activos		
Objetivo de Control		Clasificación de la información	Control	Manipulación de activos
8.2			**8.2.3**	
DESARROLLO				

Propósito

Desarrollo de procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la Unidad de Educación Virtual.

Recomendación

Una vez establecidas las directrices de clasificación de la información, es necesario ponerlas en práctica y establecer reglas para el manipulado de las mismas.

Actividades

La manipulación de los activos debe ser un proceso responsable por parte de los usuarios en pro mantener la integridad, disponibilidad e integridad de la información para ello se debe.

- Verificar los privilegios de acceso a los activos para cada persona.
- Dar a conocer la las directrices de clasificación y etiquetado adoptado por la dependencia al personal.
- Exigir el cumplimiento de los mismos.
- Monitorear el uso de los activos.

Dominio	**8**	Gestión de activos		
Objetivo de Control		Manejo de los soportes de almacenamiento.	**Control**	Gestión de soportes extraíbles.
8.3			**8.3.1**	

DESARROLLO

Propósito

Establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la Unidad de Educación Virtual.

Recomendación

Se debieran considerar los siguientes lineamientos para la gestión de medios removibles:

- Se debieran establecer los procedimientos para identificar los ítems que podrían requerir de una eliminación segura.
- Podría ser más fácil arreglar que todos los ítems de medios se recolecten y eliminen de forma segura, en lugar de tratar de separar los ítems sensibles o confidenciales.
- Cuando sea posible se debiera registrar la eliminación de ítems confidenciales

para mantener un rastro de auditoría.

Cuando se acumula medios para ser eliminados, se debiera tener en consideración el efecto de agregación, el cual puede causar que una gran cantidad de información no confidencial se convierta en confidencial.

Actividades

- Los contenidos de cualquier medio reutilizable, deben ser removidos de la institución, haciéndolos irrecuperables.
- Todos los medios deben almacenarse en un ambiente seguro de acuerdo a las especificaciones del fabricante.
- La información almacenada en medios removibles que requiera estar disponible después del tiempo de vida del medio, debe ser almacenado en cualquier otro medio de tal manera que se garantice la permanencia de la información.

Dominio	**8**	Gestión de activos		
Objetivo de Control		Manejo de los soportes de almacenamiento.	Control	Eliminación de soportes.
8.3			**8.3.2**	

DESARROLLO

Propósito

Garantizar que se eliminen de forma segura los soportes de almacenamiento una vez que ya no sean necesarios, esto a través de procedimientos formalmente establecidos.

Recomendación

- La eliminación de soportes de almacenamiento hacen referencia no solo aquellos que se encuentran en físico si también a archivos almacenados en los equipos de cómputo.
- Es importante establecer procedimientos para llevar a cabo la eliminación de dichos soportes de almacenamiento.
- Para el caso de la eliminación física se debe determinar las causas que la ameriten, ya sea estableciendo un tiempo determinado de vida útil o porque hayan dejado de funcionar; para los digitales no debe ser eliminado antes de lo establecido, es también importante que no se conserven durante más tiempo del necesario.
- En ambos casos de eliminación deben ejecutarse con procedimientos seguros que impidan una posterior recuperación y así evitar que caigan en manos de personal con malas intenciones.
-

Eliminación de documentos en papel: Para este tipo de soportes se recomienda utilizar trituradoras de papel, cuyo ancho de las tiras dependerá del grado de proyección que se desee dársele, no obstante se debe tener cuidado con el destino final de este, se

recomienda almacenar una cantidad adecuada para después de trituradas entregar al personal encargado del reciclaje.

Otro mecanismo muy efectivo es la incineración, ya que imposibilita la reconstrucción, sin embargo se debe tener mucho cuido de no ocasionar incidentes.

Eliminación de documentos electrónicos: Para este tipo de soporte se deben tener en cuenta múltiples aspectos entre ellos el lugar en que se encuentren almacenados (USB, computador, disco óptico, entre otros).

Uno de los mecanismos de eliminación es la **sobre escritura** pero no es muy confiable dado que existen formas de recuperar la información existente anteriormente, sin embargo mientras más se sobrescriba sobre ellos menor será la posibilidad de recuperación.

Para ellos existen cantidad de herramientas pagas y gratuitas, Eraser es una de ellas permite eliminar completamente los datos sensibles de su disco duro, sobrescribiendo varias veces con patrones cuidadosamente seleccionados.

Otro mecanismo es la **desmagnetización** consiste en la exposición de los soportes de almacenamiento a un campo magnético que impide la recuperación de los mismos.

Eliminación de discos duros, USB, CD entre otros: En este tipo de soportes es importante tener en cuenta que no basta solo con tirar a la basura, dado que es muy fácil para las personas con malas intenciones recuperar la información contenida en ellos aunque ya no funcionen, por ellos es importante implementar procesos de formateo definitivo para ello se puede contratar personal confiable destinado a tal fin o en caso de no ser tan alto el grado de confidencialidad se puede recurrir a herramientas para tal fin.

Para cualquiera de los casos antes mencionados es importante realizar la debida documentación.

Actividades

- Establecer tiempos de vida útil para los soportes.
- Desarrollar políticas y procedimientos para identificar y documentar la eliminación.
- Definir y documentar los métodos de eliminación de acuerdo al tipo de soporte.
- Tener a disposición programas, mecanismos o contactos con empresas confiables para realizar la eliminación segura de los soportes.
- Designar una persona responsable de vigilar la eliminación y documentar el proceso.

Dominio	**8**	Gestión de activos

Objetivo de Control	Dispositivos para movilidad y teletrabajo.	**Control**	Soportes físicos en tránsito.
8.2		**8.3.3**	

DESARROLLO

Propósito

Adoptar medidas para proteger los medios que contienen información (computadores portátiles, tabletas, discos duros, documentación impresa, externos entre otros) contra los accesos no autorizados y demás posibles riesgos a los que conlleva el mal manejo de los mismos.

Recomendación

La Unidad de Educación Virtual debe establecer procedimientos seguros para la manipulación de activos fuera de los límites de la dependencia o de la institución, tanto aquellos se me manejan físicamente como aquellos que se encuentren en diferentes medios como CD, USB, discos duros, computadores, tabletas, entre otros.

Actividades

- Determinar qué tipo de uso se puede dar a los mismos fuera de la dependencia.
- En caso de equipos de cómputo se debe establecer los requisitos de seguridad mínimos con que debe contar un equipo de cómputo.
  a) Software antivirus.
  b) Contraseña de Acceso
  c) Control de acceso a las redes
- Delegar un responsable de verificar el cumplimiento de estas políticas de seguridad para los soportes físicos cuando se encuentran fuera de las instalaciones de la dependencia cada vez que se haga uso de los mismos.
- Cada vez que se pongan en tránsito dichos soportes se debe realizar la debida documentación, en lo posible llevar un formato con las especificaciones necesarias.

Dominio	**9**	Control de accesos		
Objetivo de Control		Requisitos del negocio para el control de acceso	**Control**	Política de control de acceso
9.1			9.1.1	

DESARROLLO

Propósito

Establecer y documentar mecanismos de control de accesos en base a las necesidades de la Unidad de Educación Virtual para la gestión segura de la plataforma Moodle de apoyo a la presencialidad.

Recomendación

Es importante establecer procedimientos formales de acceso a la información y las aplicaciones a través de las cuales se realiza la gestión de la misma, lo que implica la revisión, modificación y evaluación.

Actividades

a) Teniendo en cuenta las directrices de clasificación de la información dispuestas para el control 8.2, se deben establecer los requerimientos de seguridad para las categorías establecidas.
b) Definir los posibles riesgos y amenazas y clasificarlos según su impacto.
c) Establecer mecanismos para contrarrestarlos
d) Definir detalladamente los perfiles de acceso de los usuarios.
e) Administrar los privilegios de acceso según el tipo de usuario.
f) Definir controles de obligatorio cumplimientos, entre ellos los siguientes:
    - Registro de acceso
    - Uso de contraseñas seguras.
    - Tiempo de inactividad de la sesión.
    - Limitar los tiempos de conexión.
    - No permitir la instalación de ningún programa no autorizado
    - No conectarse a través de redes públicas.
g) Elaborar el documento.

Dominio	**9**	Control de accesos		
Objetivo de Control		Requisitos de negocio para el control de accesos	**Control**	Control de acceso a las redes y servicios asociados.
9.1			**9.1.2**	

DESARROLLO

Propósito

Restringir la capacidad de los usuarios para conectarse a la red, en línea con la política de control de acceso y los requerimientos de las aplicaciones.

Recomendación

Los derechos de acceso a la red de los usuarios se deberían mantener y actualizar según se requiera a través de la política de control de acceso.

Actividades

Restringir la capacidad de conexión de los usuarios a través de Gateway de la red que filtra el tráfico por medio de tablas o reglas predefinidas. Los ejemplos de aplicaciones a las cuales se pueden aplicar las restricciones son:

- Mensajes; por ejemplo, correo electrónico.
- Transferencia de archivos.

- Acceso interactivo.
- Acceso a una aplicación.

Dominio	**9**	Control de acceso		
Objetivo de Control		Gestión de acceso de usuario.	Control	Gestión de altas bajas/bajas en el registro de usuarios.
9.2			**9.2.1**	

DESARROLLO

Propósito

Establecer un proceso formal de registro y anulación de usuario para la asignación de derechos de acceso.

Recomendación

Se debe otorgar derechos de acceso al personal responsable directamente con la gestión manejada a través de la plataforma de apoyo a la presencialidad, con el fin que pueda acceder a la información necesaria para el desempeño de sus funciones, de igual manera se debe eliminar el identificador de un usuario una vez se desvincule de su labor.

Actividades

- Crear un formulario con los campos necesarios para otorgar permisos de acceso o para eliminarlos.
- Dar a conocer el formato para que sea utilizado para solicitar un alta o baja.
- Dado que la plataforma funciona para fines educativos, la mayoría de los usuarios son docentes y estudiantes, por lo que el administrador de la plataforma debe monitorear frecuentemente la vinculación de los mismos con la institución para determinar si aún deben mantener los privilegios de acceso asignados o si se debe modificar o inclusive dar de baja.

Dominio	**9**	Control de acceso		
Objetivo de Control		Gestión de acceso de usuario.	Control	Gestión de los derechos de acceso asignados a usuarios.
9.2			**9.2.2**	

DESARROLLO

Propósito

Revisar los derechos de acceso de los usuarios que ingresan a la Plataforma de Apoyo a la Presencialidad.

Recomendación

Se recomienda establecer claramente los permisos con los cuales cuenta cada rol dentro de la plataforma, para asegurar el buen uso de la misma.

Actividades

- Definir los derechos de acceso de los usuarios que harán parte de la plataforma de apoyo a la presencialidad.
- Establecer los permisos con los que cuenta cada rol dentro de la plataforma

Dominio	**9**	Control de acceso	
Objetivo de Control	Gestión de acceso de usuario.	Control	Gestión de los derechos de acceso con privilegios especiales.
9.2		**9.2.3**	

DESARROLLO

Propósito

Establecer los derechos de acceso y permisos a usuarios con privilegios especiales

Recomendación

Se recomienda establecer los permisos para roles privilegiados, como lo son el administrador de la plataforma y los docentes.

Actividades

- Definir los permisos al administrador de la plataforma de apoyo a la presencialidad.
- Definir los permisos a los docentes que cuentan con cursos en la plataforma de apoyo a la presencialidad.
- Definir los permisos para el rol estudiante.

Dominio	**9**	Control de acceso	
Objetivo de Control	Gestión de acceso de usuario.	Control	Gestión de información confidencial de autenticación de usuarios.
9.2		**9.2.4**	

DESARROLLO

Propósito

Gestionar la información confidencial de la autenticación de usuarios.

Recomendación

La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.

La asignación de la información secreta de autenticación se controla a través de un proceso de gestión formal y de acuerdo a la clasificación dada a los activos por parte de los responsables.

Dominio	**9**	Control de accesos		
Objetivo de Control		Gestión de acceso a usuario	Control	Revisión de los derechos de acceso de los usuarios.
9.2			**9.2.5**	

DESARROLLO

Propósito

Inspeccionar los derechos de acceso de los usuarios a intervalos regulares utilizando un procedimiento formal.

Recomendación

- Revisar los derechos de acceso de los usuarios a intervalos de 4 a 6 meses y cuando haya cualquier cambio, asenso, cambio de puesto, terminación del contrato.
- Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 3 meses aproximadamente
- Revisar las asignaciones de privilegios a intervalos de en periodos no mayor a 6 meses, a fin de garantizar que no se obtengan privilegios no autorizados.
- Se debieran registrar los cambios en las cuentas privilegiadas para una revisión periódica.

Actividades

Revisar regularmente los derechos de acceso de los usuarios para mantener un control efectivo sobre el acceso a la data y los servicios de información.

Dominio	**9**	Control de accesos		
Objetivo de Control		Gestión de acceso a usuario	Control	Retirada o adaptación de los derechos de acceso

9.2		**9.2.6**	

DESARROLLO

Propósito

Remover los derechos de acceso de todos los usuarios funcionarios, personal a honorarios y terceras personas a la información y los medios de procesamiento de información como consecuencia de su desvinculación, o deberían ser ajustados si sus funciones cambian.

Recomendación

En la terminación del contrato debiera retirarse los derechos del individuo los activos asociados con los sistemas y servicios de información tras la desvinculación.
En caso de cambio de un empleo deben removerse todos los derechos de acceso que no fueron aprobados para el nuevo empleo, tales como: accesos lógicos y físicos, llaves, tarjetas de identificación, instalaciones de procesamiento de la información, suscripciones, y remoción de cualquier documentación que lo identifique como un miembro corriente del Organismo.
Si un empleado, contratista o usuario de tercera parte que se está desvinculando tiene conocimiento de contraseñas para cuentas que permanecen activas, éstas deben ser cambiadas tras la finalización o cambio de empleo, contrato o acuerdo.

Actividades

Crear un procedimiento de baja de usuarios en los sistemas de información,
que considere la revocación de sus cuentas de acceso dependiendo de los siguientes factores de riesgo:

- Cuando el termino o cambio de trabajo, es iniciado por el funcionario o contratista, o por razones administrativas.
- Las responsabilidades actuales del funcionario o contratista.
- Valor de los activos que actualmente maneja.

Dominio	**9**	**Control de accesos**	
Objetivo de Control	**Responsabilidades de usuario**	**Control**	Uso de información confidencial para la autentificación.
9.3		9.3.1	

DESARROLLO

Propósito

Establecer la obligatoriedad a todos los usuarios del uso de información confidencial para la autenticación.

Recomendación

Dado que inicialmente a los usuarios se les genera una contraseña de acceso a través del sistema, posteriormente cuentan con total libertad de realizar el cambio de la misma, dada esta circunstancia es importante concientizar a los usuarios de las responsabilidades asignas respecto a la seguridad de la información.

Actividades

A) Dar conocer a todos los usuarios la importancia de mantener las tres características más importantes de la información (integridad, disponibilidad y confiablidad).
B) Recordar que cada uno de los tipos de usuario tienen asignados ciertos privilegios, por lo nadie más debería poder acceder a la plataforma a través de claves que no le pertenezcan.
C) Recordarles que una vez identificados en el sistema (loguearse) todas las acciones realizadas con ese nombre de usuario serán su responsabilidad aunque sea otra persona la que haya ingresado con su usuario.
D) Capacitar sobre las recomendaciones para mantener la confidencialidad de las contraseñas.
E) No permitir que ningún usuario ingrese a la plataforma con una contraseña no propia.

Dominio	**9**	**Control de accesos**		
Objetivo de Control		**Control de acceso a sistemas y aplicaciones.**	**Control**	Restricción de acceso a la información.
9.4			9.4.1	

DESARROLLO

Propósito

Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

Recomendación

Al ser la información el activo más importante, se debe limitar el acceso a la misma, establecer mecanismos que permitan mantener su confidencialidad.

Actividades

- Según la clasificación realizada se debe determinar el nivel de seguridad requerido para la gestión de la información.
- Para aquella información confidencial, como es el caso de contraseña de acceso, reportes de notas, copias de seguridad etc, se debe asignar un mayor grado de seguridad dado que cualquier persona no puede tener acceso a ella, en ese caso de deben implementar, para archivos digitales contraseñas de acceso y para el caso de documentos en físico almacenar en archivadores bajo llaves.
- Realizar una buena gestión de contraseñas y de llaves de acceso, determinar responsablemente que persona o personas serán las encargadas de las mismas.
- Identificar los tipos de usuarios existentes y los privilegios asignados.
- Implementar controles de autentificación.
- Cerciorarse mediante auditorias y controles de acceso físico que solo el personal autorizado pueda acceder a la información.

Dominio	**9**	Control de accesos		
Objetivo de Control		Control de acceso a sistemas y aplicaciones	**Control**	Procedimientos seguros de inicio de sesión
9.4			9.4.2	

DESARROLLO

Propósito

Controlar el acceso a los sistemas operativos mediante un procedimiento de registro seguro.

Recomendación

El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado.

Actividades

Diseñar un registro que cumpla con los siguientes aspectos:

- No debería mostrar identificadores del sistema o aplicación hasta que se haya completado satisfactoriamente el proceso de registro.
- Debería mostrar la advertencia general que a la computadora sólo pueden tener acceso los usuarios autorizados.
- No debería proporcionar mensajes de ayuda durante el procedimiento de registro que ayuden al usuario no autorizado.
- Debería limitar el número de intentos de registro infructuosos permitidos; por ejemplo, tres intentos.

- No debería mostrar la clave secreta que se está ingresando o considerar esconder los caracteres de la clave secreta mediante símbolos.
- No debería transmitir claves secretas en un texto abierto a través de la red.

Dominio	**9**	Control de accesos		
Objetivo de Control		Control de acceso a sistemas y aplicaciones	**Control**	Gestión de contraseñas de usuarios
9.4			9.4.3	

DESARROLLO

Propósito

Definir mecanismos para implementar contraseñes seguras con el propósito de proteger de accesos no autorizados a la información manejada a través de los equipos de cómputo.

Recomendación

Las contraseñas son una serie de caracteres que desbloquean el acceso a equipos de cómputo o a software, la función de las contraseñas es evitar accesos no autorizados y proteger la información.

A través de la plataforma Moodle, se manejan varios tipos de usuario cada uno de ellos con diferentes privilegios, la responsabilidad de gestionar dichas contraseñas corresponde al administrador; es importante para este proceso de asignación de contraseñas se implementen mecanismo que permitan darles el mayor grado de protección.

Hace poco tiempo la universidad realizó el proceso de unificación de contraseñas para todos los usuarios, es decir que para acceder a cualquiera de los sistemas que maneja la universidad se debe hacer a través de una única contraseña, incluyendo el acceso a la plataforma Moodle de apoyo a la presencialidad; existen ciertas recomendaciones para que los usuarios utilicen contraseñas seguras estas son:

- Deben estar conformadas por mínimo 10 caracteres.
- Los caracteres deben estar mezclados entre números y letras.
- Debe existir por lo menos un carácter en mayúscula.

Estas son recomendaciones valiosas sin embargo, es importante que no se remitan solo a ser recomendaciones sino que sean de obligatorio cumplimiento.

Aparte de las recomendaciones ya mencionadas existen otras que al ser tomadas en cuenta permitirán aumentar considerablemente el grado de seguridad.

Actividades

- Tener en cuenta las siguientes pautas para la asignación de contraseñas seguras:

  a) Cuanto más fácil sea de recordar una contraseña, más fácil será para una persona mal intencionada adivinarla, por lo que se recomienda que no se utilicen palabras o números obvios, por ejemplo no se recomienda utilizar como contraseñas fechas, como cumpleaños, aniversarios entre otras, tampoco nombres, ni números en secuencia.

  b) Como mínimo se recomienda que las contraseñas estén compuestas por 8 caracteres entre números y letras, pero nunca utilizar solo números o solo letras, siempre mezclados.

  c) No utilizar información personal, dado que si una persona tiene intenciones de violar su privacidad, lo primero que haría sería investigar acerca de usted por lo que sería fácil adivinar su contraseña.

  d) Nunca escriba su contraseña en papel, ni en ningún archivo físico o digital, siempre será más seguro memorizarla.

  e) Para darle más seguridad a la contraseña puede reemplazar algunos caracteres por símbolos.

- Dado que la asignación de la contraseña es de escogencia libre por cada usuario se deben validar las mismas para hacer obligatoriedad del cumplimiento de las ya definidas.
- Buscar mecanismos de comunicación que permitan incentivar al estudiante sobre el uso de las recomendaciones en mención para establecer una contraseña segura, para ello se recomienda realizar capacitaciones o mostrar la información en la página institucional o en interfaces principales de la plataforma a través de recursos llamativos, como por ejemplo una animación.

Dominio	**9**	Control de accesos		
Objetivo de Control		Responsabilidades de usuario	**Control**	Uso de herramientas de administración de sistemas.
9.4			9.4.4	
DESARROLLO				

Propósito Gestionar el uso de herramientas de administración del sistema.
Recomendación Se recomienda utilizar herramientas para la administración de los servidores.
Actividades Utilizar herramientas acordes para la administración de los servidores en los que se encuentra alojada la plataforma.

Dominio	**10**	Cifrado	
Objetivo de Control	Controles criptográficos	**Control**	Política de uso de los controles criptográficos.
10.1		**10.1.1**	

DESARROLLO

Propósito

Desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.

Recomendación

Cuando se desarrolla una política criptográfica se debe considerar lo siguiente:

- El enfoque gerencial sobre el uso de los controles criptográficos a través de la organización, incluyendo los principios generales bajo los cuales se debe proteger la información comercial.
- El uso de codificación para la protección de la información confidencial transportada por los medios y dispositivos móviles o removibles o a través de las líneas de comunicación.
- El enfoque de la gestión de claves, incluyendo los métodos para lidiar con la protección de las claves criptográficas y la recuperación de la información codificada en el caso de claves perdidas, comprometidas o dañadas.
- Roles y responsabilidades; por ejemplo, quién es responsable de la implementación de la política.
- Gestión de claves, incluyendo la generación de claves.

Actividades

Utilizar controles criptográficos en los siguientes casos:
1. Para la protección de claves de acceso a sistemas, datos y servicios.
2. Para la transmisión de información clasificada, fuera de la Institución.

Dominio	**10**	**Cifrado**		
Objetivo de Control		**Controles criptográficos**	**Control**	Gestión de claves
10.1			**10.1.2**	

DESARROLLO

Propósito

Establecer la gestión de claves para dar soporte al uso de técnicas criptográficas en la organización.

Recomendación

Todas las claves criptográficas deben estar protegidas contra una modificación, pérdida y destrucción. Además, las claves secretas y privadas necesitan protección contra la divulgación no autorizada.
Se debe proteger físicamente el equipo utilizado para generar, almacenar y archivar las claves.
El sistema de gestión de claves se debe basar en un conjunto de estándares, procedimientos y métodos seguros acordados para:

- Generar claves para los diferentes sistemas criptográficos y las diversas aplicaciones.
- Generar y obtener certificados de claves públicas.
- Distribuir claves a los usuarios planeados, incluyendo cómo se debieran activar las claves una vez recibidas.
- Revocar las claves incluyendo cómo se debe retirar o desactivar las claves; por ejemplo, cuando las claves se han visto comprometidas o cuando el usuario deja la organización.
- Recuperar las claves cuando han sido perdidas o corrompidas como parte de la continuidad y gestión del negocio.
- Destruir las claves.
- Registrar y auditar las actividades relacionadas con la gestión de claves.

Para poder reducir la posibilidad de comprometer las claves, se debe definir las fechas de activación y desactivación para que las claves sólo se puedan utilizar durante un período de tiempo limitado. El período de tiempo dependerá de las circunstancias bajo las cuales se está utilizando el control criptográfico, y el riesgo percibido.

Actividades

- Considerar la autenticidad de las claves públicas. Este proceso de autenticación se puede realizar utilizando certificados de claves públicas, los cuales normalmente son emitidos por una autoridad de certificación, la cual debe ser una organización reconocida con controles y procedimientos adecuados para proporcionar el grado de confianza requerido.

- Abarcar los temas de responsabilidad, confiabilidad de los servicios y tiempos de respuesta para la provisión de los servicios.

Dominio	**11**	Seguridad física y ambiental		
Objetivo de Control		Áreas seguras	**Control**	Perímetro de seguridad física
11.1			**11.1.1**	

DESARROLLO

Propósito

Utilizar los perímetros de seguridad para proteger las áreas que contengan información y recursos para su procesamiento.

Recomendación

- Los perímetros de seguridad deben estar claramente definidos, y la ubicación y fuerza de cada uno de los perímetros dependerá de los requerimientos de seguridad de los activos dentro del perímetro y los resultados de la evaluación del riesgo.
- Los perímetros del área que contienen los medios de procesamiento de información deben ser físicamente sólidos.
- Las paredes externas del local deben ser una construcción sólida y todas las puertas externas deben estar adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control.
- Las puertas y ventanas deben quedar aseguradas cuando están desatendidas y considerar una protección externa.
- El área debe contar con una recepción o un(a) recepcionista u otros medios para controlar el acceso físico al área; el acceso al área debe ser restringida solamente al personal autorizado.
- Todas las puertas de emergencia en un perímetro de seguridad debieran contar con alarma, ser monitoreadas y probadas en conjunción con las paredes para establecer el nivel de resistencia requerido en concordancia con los adecuados estándares regionales, nacionales e internacionales.
- Se debe operar en concordancia con el código contra incendios local de una manera totalmente segura.
- Instalar adecuados sistemas de detección de intrusos según estándares nacionales, regionales e internacionales, probados regularmente para abarcar todas las puertas externas y ventanas accesibles.
- Las áreas no ocupadas deben contar con alarma en todo momento.
- Proveer protección para otras áreas; por ejemplo, el cuarto de cómputo o cuarto

de comunicaciones.

- Los medios de procesamiento de información manejados por la organización deben estar físicamente separados de aquellas manejadas por terceros.

Actividades

- Definir y documentar claramente los perímetros de seguridad de acuerdo a la ubicación y requerimientos de seguridad de los activos.
- Ubicar las instalaciones de procesamiento de información dentro del perímetro del área de construcción físicamente sólida.
- Instalar alarmas a las puertas de emergencia en un perímetro de seguridad
- Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área.

Dominio	**11**	Seguridad física y ambiental		
Objetivo de Control		Áreas seguras	**Control**	Controles físicos de entrada
11.1			11.1.2	

DESARROLLO

Propósito

Proteger las áreas seguras mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.

Recomendación

- La fecha y la hora de entrada y salida de los visitantes debe ser registrada y todos los visitantes deben ser supervisados a no ser que su acceso haya sido previamente aprobado.
- Sólo se le debe permitir acceso por propósitos específicos y autorizados a visitantes y se deben emitir las instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia.
- El acceso a áreas donde se procesa o almacena información sensible debe ser controlada y restringida sólo al personal autorizado.
- Se debe utilizar controles de autenticación; por ejemplo, tarjeta de control de acceso más PIN; para autorizar y validar todo los accesos; se debiera mantener un rastro de auditoría de todos los accesos.
- Para todos los usuarios empleados, contratistas y terceras personas y todos los visitantes deben usar como requisito alguna forma de identificación visible.
- Al personal de servicio de apoyo de terceros se le debe otorgar acceso restringido

las áreas seguras o los medios de procesamiento de información confidencial, sólo cuando sea necesario; este acceso debe ser autorizado y monitoreado.
- Los derechos de acceso a áreas seguras deben ser revisados y actualizados regularmente, y revocados cuando sea necesario.

Actividades

- Establecer requerimientos de seguridad del área y los procedimientos de emergencia, para autorizar e instruir al visitante en el momento que se le permita el ingreso.
- Supervisar o inspeccionar a los visitantes a áreas protegidas.
- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.
- Diseñar controles de autenticación para autorizar y validar todos los accesos.
- Mantener un registro protegido que permita auditar todos los accesos.
- Implementar el uso de una identificación unívoca visible para todo el personal del área protegida.
- Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

Dominio	**11**	Seguridad física y ambiental		
Objetivo de Control		Áreas seguras	**Control**	Seguridad de oficinas, despachos y recursos.
11.1			11.1.3	

DESARROLLO

Propósito

Diseñar estrategias y mecanismos de seguridad física para la oficina de la Unidad de Educación Virtual de la UFPSO.

Recomendación

Dado que actualmente la oficina no se encuentra en un lugar adecuado, es importante idear mecanismos que le permitan bridar el máximo grado de protección posible a la información que se maneja desde la dependencia.

Actividades

a) Todo el material con información física que se maneje en la dependencia debe almacenarse en lugares seguros como casilleros bajo llave.
b) Los Rack deben contar con candados de seguridad.
c) Los equipos de cómputo deben contar con contraseñas de acceso.

d) Capacitar al personal en cuanto al uso de contraseñas seguras, la importancia de mantener la confidencialidad de la información.
e) Verificar que los equipos de cómputo cuenten con mecanismos de protección contra software malicioso y que se realicen mantenimientos tanto correctivos como preventivos frecuentemente, de lo contrario realizar la solicitud correspondiente a la dependencia encargada.

Dominio **11**	Seguridad física y ambiental		
Objetivo de Control	Áreas seguras	**Control**	Protección contra las amenazas externas y ambientales
11.1		**11.1.4**	

DESARROLLO

Propósito

Definir estrategias de protección física contra desastres naturales, ataques maliciosos o accidentes.

Recomendación

La Unidad Virtual por ser una dependencia de la universidad podrá regirse por los planes de contingencia existentes en la Universidad para protegerse contra amenazas externas y ambientales, por lo que el personal debe conocer a cabalidad dicho plan y saber cómo actuar en caso de presentarse incidentes como los planteados en el mismo, para esto es importante apoyase del personal responsable establecido por los directivos de la Universidad.

Actividades

A) La coordinación de la Unidad debe solicitar capacitaciones para todo el personal acerca de los planes de contingencia que existen en la Universidad en caso de presentarse desastres naturales o incidentes similares (incendios, inundaciones, revueltas civiles, entre otros).

B) Acatar los controles establecidos en la política de seguridad de la UFPSO, capitulo dos artículo décimo cuarto, en el que se establecen los siguientes mecanismos para preservar la seguridad física y del medio ambiente:

• En los centros de cómputo o áreas que la entidad considere criticas deberán existir elementos de control de incendio y alarmas.

• En lo referente a la ubicación de computadores y hardware en general, se debe tener especial cuidado contra fallas del sistema de control del medio ambiente, y otras amenazas que puedan afectar la normal operación del sistema.

• En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo indicio de incendio. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses.

• Se deben tener extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales.

• El cableado de la red debe ser protegido de interferencias usando canaletas que lo protejan.

• Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

Dominio	**11**	Seguridad física y ambiental		
Objetivo de Control		Áreas seguras	**Control**	El trabajo en áreas seguras
11.1			11.1.5	

DESARROLLO

Propósito

Definir las medidas para garantizar la seguridad en áreas de trabajo.

Recomendación

Desde las instalaciones de la Unidad de Educación Virtual se administra información importante entre ellas la gestionada a través la plataforma Moodle de apoyo a la presencialidad, esta información se considera sensible, por lo que el manejo de la misma debe realizarse en áreas seguras.

Dado que esta oficina no se encuentra ubicada en el sitio adecuado, se recomienda solicitar cambio de instalaciones y asegurarse de que se cumplan las medidas establecidas en la política de seguridad de la UFPSO capitulo II, artículo décimo séptimo para la nueva ubicación de las mismas.

Actividades

a) Las centrales de conexión o centros de cableado no deben estar ubicadas en el espacio correspondiente a las áreas de trabajo, debe existir una delimitación adecuada.

b) La estación de trabajo del administrador de plataforma debe tener acceso restringido y contar con cámaras de seguridad.

c) La oficina debe estar equipada con todos los implementos necesarios de protección contra fuego, terremotos, temblores, explosiones, revoluciones civiles y otras formas de desastres naturales o de naturaleza humana.

d) Se deben realizar inspecciones periódicas de seguridad física de las instalaciones.

Dominio	11	Seguridad física y ambiental		
Objetivo de Control		Seguridad de los equipos	**Control**	Emplazamiento y protección de equipos
11.2			**11.2.1**	

DESARROLLO

Propósito

Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la Institución.
Proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no autorizado.

Recomendación

a) Ubicar el equipo de manera que se minimice el acceso innecesario a las áreas de trabajo.
b) Los medios de procesamiento de la información que manejan información confidencial deben ubicarse de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso.
c) Asegurar los medios de almacenaje para evitar el acceso no autorizado.
d) Aislar los ítems que requieren protección especial para reducir el nivel general de la protección requerida.
e) Adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.
f) Establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información.
g) Monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información.
h) Aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.
i) Proteger el equipo que procesa la información confidencial para minimizar el

riesgo de escape de información debido a emanación.

Actividades

- Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
- Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
- Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará en un periodo no mayor a seis meses.
- Aplicar protección contra rayos a todos los edificios y se deben adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.

Dominio	11	Seguridad física y ambiental		
Objetivo de Control		Seguridad de los equipos	**Control**	Instalaciones de suministro
11.2			**11.2.2**	

DESARROLLO

Propósito

Proteger los equipos de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.

Recomendación

a) Todos los servicios públicos de soporte; como electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado; deben ser adecuados para los sistemas que soportan.
b) Los servicios públicos de soporte deben ser inspeccionados regularmente y conforme sea apropiado, probados para asegurar su adecuado funcionamiento y para reducir cualquier riesgo por un mal funcionamiento o falla.
c) proveer un suministro eléctrico adecuado que esté de acuerdo a las especificaciones del fabricante del equipo.
d) Se recomienda un dispositivo de suministro de energía ininterrumpido (UPS) para apagar o el funcionamiento continuo del equipo de soporta las operaciones comerciales críticas.
e) Los planes de contingencia para la energía debieran abarcar la acción a tomarse en el caso de una falla de energía prolongada.
f) considerar un generador de emergencia si se requiere que el procesamiento continué en el caso de una falla de energía prolongada.
g) Se debe tener disponible un adecuado suministro de combustible para asegurar que el generador pueda funcionar durante un período prolongado.
h) El equipo UPS y los generados se deben chequear regularmente para asegurar que

tengan la capacidad adecuada y para probar su concordancia con las recomendaciones del fabricante.

i) se debe considerar al uso de múltiples fuentes de energía, si el área es grande, una subestación de energía separada.
j) Los interruptores de energía de emergencia se deben colocar cerca de las salidas de emergencia en las habitaciones donde se encuentra el equipo para facilitar el cierre del paso de corriente en caso de una emergencia.
k) proporcionar iluminación de emergencia en caso de una falla en la fuente de energía principal.
l) El suministro de energía debe ser estable y adecuado para suministrar aire acondicionado, equipo de humidificación y los sistemas contra-incendios (donde se utilicen).
m) Se debiera evaluar e instalar, si se requiere, un sistema de alarma para detectar mal funcionamiento en los servicios públicos de soporte.
n) El equipo de telecomunicaciones se debiera conectar al proveedor del servicio mediante por lo menos dos rutas para evitar que la falla en una conexión evite el desempeño de los servicios de voz.
o) Los servicios de voz deben ser adecuados para cumplir con los requerimientos legales de las comunicaciones de emergencia.

Actividades

- Diseñar planes de contingencia que permitan contemplar las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS deberán ser inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
- Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía.
- Implementar protección contra descargas eléctricas en todas las áreas y líneas de comunicaciones externas de acuerdo a las normativas vigentes para cuando se presente una falla en el suministro principal de energía.

Dominio	11	Seguridad física y ambiental		
Objetivo de Control		Seguridad de los equipos	**Control**	Seguridad del cableado
11.2			**11.2.3**	

DESARROLLO

Propósito

Proteger contra la intercepción o daño el cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información.

Recomendación

- Cuando sea posible, las líneas de energía y telecomunicaciones que van a los medios de procesamiento de información deben ser subterráneas o estar sujetas a una alternativa de protección adecuada.
- Los cables de energía debieran estar separados de los cables de comunicaciones para evitar la interferencia
- Utilizar marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados
- Utilizar una lista de empalmes documentados para reducir la posibilidad de error.
- Para sistemas sensibles o críticos se debe considerar más controles como:
- la instalación de un tubo blindado y espacios o cajas con llave en los puntos de inspección y terminación;
- el uso de rutas alternativas y/o medios de transmisión proporcionan una seguridad adecuada;
- el uso de cableado de fibra óptica;
- el uso de un escudo electromagnético para proteger los cables;
- la iniciación de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se adhieran a los claves;
- acceso controlado para empalmar los paneles y los cuartos de cableado.

Actividades

- Proteger contra intercepciones no autorizadas o daños el cableado de la red, por ejemplo, utilizando un tubo o evitando las rutas a través de áreas públicas.
- Rotular o marcar adecuadamente los cables para reducir al mínimo los errores de manejo.
- Separar los cables de energía de los cables de comunicación para evitar interferencia
- Realizar barridos técnicos e inspecciones físicas contra dispositivos no autorizados conectados a los cables.

Dominio	11	Seguridad física y ambiental		
Objetivo de Control		Seguridad de los equipos	**Control**	Mantenimiento de los equipos
11.2			**11.2.4**	

DESARROLLO

Propósito

Mantener correctamente los equipos para asegurar su continua disponibilidad e integridad.

Recomendación

a) El equipo se debe mantener en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor.
b) Sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo.
c) Mantener registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo.
d) Implementar los controles apropiados cuando se programa el equipo para mantenimiento, tomando en cuenta si su mantenimiento es realizado por el personal en el local o fuera de la organización; cuando sea necesario y revisar la información confidencial del equipo, o se debiera verificar al personal de mantenimiento.

Actividades

- Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área.
- Llevar un registro actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- Registrar el retiro de equipamiento de la sede del Organismo para su mantenimiento.
- Eliminar la información confidencial que contenga cualquier equipamiento, realizándose previamente las respectivas copias de resguardo antes de que se vayan a llevar el equipo para hacer mantenimiento.

Dominio	11	Seguridad física y ambiental		
Objetivo de Control		Seguridad de los equipos	**Control**	Reutilización o retirada segura de dispositivos de almacenamiento.
11.2			**11.2.7**	

DESARROLLO

Propósito

Chequear los ítems del equipo que contiene medios de almacenaje para asegurar que se haya retirado o sobre-escrito cualquier data confidencial o licencia de software antes de su eliminación.

Recomendación

Los dispositivos que contienen información confidencial deben ser físicamente destruidos o se debieran destruir, borrar o sobre escribir la información utilizando técnicas que hagan imposible recuperar la información original, en lugar de simplemente utilizar la función estándar de borrar o formatear.

Los dispositivos que contienen data confidencial pueden requerir una evaluación del

riesgo para determinar si los ítems deben ser físicamente destruidos en lugar de enviarlos a reparar o descartar.
Actividades Diseñar e implementar procedimientos de borrado seguro de datos y de reutilización de equipos.

Dominio	11	Seguridad física y ambiental		
Objetivo de Control		Seguridad de los equipos	**Control**	Equipo informático de usuario desatendido.
11.2			**11.2.8**	
DESARROLLO				
Propósito Asegurar que los equipos desatendidos sean protegidos apropiadamente.				
Recomendación • Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña. • Proteger los equipos o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.				
Actividades Coordinar con el Área de Personal las tareas de concienciación a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos.				

Dominio	11	Seguridad física y ambiental		
Objetivo de Control		Seguridad de los equipos	**Control**	Política de puesto de trabajo despejado y bloqueo de pantalla
11.2			**11.2.9**	
DESARROLLO				
Propósito La política de puesto de trabajo despejado y pantalla limpia reduce los riesgos de accesos no autorizados, perdida o daño de la información durante las horas normales de trabajo Mantener el lugar de trabajo sin información que pueda causar futuros daños.				

Recomendación

- La información confidencial o crítica; por ejemplo, en papel o medios de almacenamiento electrónicos; debiera ser guardada bajo llave, cuando no está siendo utilizada, especialmente cuando la oficina está vacía.
- Cuando se dejan desatendidas, las computadoras y terminales debieran dejarse apagadas o protegidas con mecanismos para asegurar la pantalla y el teclado, controlados mediante una clave secreta, dispositivo o un mecanismo de autenticación de usuario similar y se debieran proteger con llave, claves secretas u otros controles cuando no están en uso.
- Se debieran proteger los puntos de ingreso y salida de correo y las máquinas de fax desatendidas.
- Los documentos que contienen información confidencial o clasificada debieran sacarse inmediatamente de la impresora.

Dominio	**12**	**Seguridad en la Operativa**		
Objetivo de Control		Responsabilidades y procedimientos de operación.	**Control**	Documentación de procedimientos de operación.
12.1			**12.1.1**	

DESARROLLO

Propósito

Documentar, mantener y poner a disposición los procedimientos de operación de todos los usuarios, a quien lo necesite.

Recomendación

a) Preparar procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información; tales como procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento de los equipos y seguridad.

b) Los procedimientos de operación deben especificar las instrucciones para la ejecución detallada de cada trabajo incluyendo:

- Procesamiento y manejo de información.
- Copia de seguridad.
- Soporte en el evento de dificultades operacionales o técnicas Inesperadas.
- Procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema.

Actividades

- Documentar y mantener actualizados los procedimientos operativos identificados y sus cambios serán autorizados por el responsable de Seguridad de la Información.
- Diseñar y establecer procedimientos para la operación de la infraestructura que incluya:

-Manejo y procedimiento de la información
-Respaldos
-Requerimientos de tareas automatizadas, incluyendo las dependencias con otros sistemas.
-Alertas sobre tareas ejecutadas correcta e incorrectamente.
-Reinicio de sistemas y procedimientos de recuperación ante fallas de los sistemas.
-Procedimientos de la administración de logs de la plataforma moodle.

- Documentar las siguientes actividades:

-Instalación y mantenimiento de la Plataforma Moodle de Apoyo a la Presencialidad
-Monitoreo del procesamiento.
-Resguardo de información.

Dominio	**12**	**Seguridad en la Operativa**		
Objetivo de Control		Responsabilidades y procedimientos de operación.	**Control**	Gestión de cambios
12.1			**12.1.2**	

DESARROLLO

Propósito

Controlar los cambios en la Plataforma Moodle de Apoyo a la Presencialidad.

Recomendación

- La Plataforma de Apoyo a la Presencialidad y los sistemas de procesamiento de información deben estar sujetos a un estricto control del cambio.
- El control inadecuado de los cambios en los sistemas es una causa común de fallas en el sistema o en la seguridad.
- Los cambios en la versión de la Plataforma, pueden influir en la confiabilidad de la aplicación.
- Los cambios sólo se deben realizar cuando existe una razón válida para hacerlo.
- Actualizar los sistemas con la versión más moderna no es siempre lo mejor, ya que podría introducir más vulnerabilidades e inestabilidad que la versión actual.

Actividades

- Definir y establecer procedimientos para el control de los cambios en el ambiente operativo. Estos procedimientos deben contemplar:

a) Identificación y registro de cambios significativos.
b) Planeación y prueba de cambios.
c) Evaluación de los impactos potenciales de los cambios, incluyendo los impactos de seguridad.
d) Procedimiento de aprobación formal para los cambios propuestos.
e) Comunicación de los detalles del cambio para todas las personas relevantes:
f) Procedimientos de emergencia y respaldo, incluyendo los procedimientos y responsabilidades para abortar y recuperarse de cambios fallidos y eventos inesperados.

Dominio	**12**	**Seguridad en la Operativa**		
Objetivo de Control		Responsabilidades y procedimientos de operación.	**Control**	Gestión de Capacidades
12.1			**12.1.3**	

DESARROLLO

Propósito

Monitorear, mejorar el uso de los recursos y realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido de la Plataforma Moodle de Apoyo a la Presencialidad.

Recomendación
Se debe identificar los requerimientos de capacidad de cada actividad nueva y en proceso; además, se debe monitorear la plataforma para asegurar y, cuando sea necesario, mejorar la disponibilidad y eficiencia de la plataforma.
Se deben establecer detectives de controles para indicar los problemas en el momento debido.

Actividades
Llevar informes periódicos del uso de las capacidades de la plataforma, de tal manera que se pueda obtener un estimado de su rendimiento y capacidad máxima sin degradar los servicios.

Dominio	**12**	**Seguridad en la Operativa**		
Objetivo de Control		Protección contra código malicioso	**Control**	Controles contra el código malicioso.
12.2			**12.2.1**	

DESARROLLO

Propósito
Controles de detección, prevención y recuperación para proteger contra códigos maliciosos.

Recomendación
El Responsable de Seguridad de la Información debe definir controles de detección y prevención para la protección contra software malicioso y concientizar a los usuarios en materia de seguridad, controles de acceso a la plataforma y administración de cambios. El Responsable del Área Informática, o el personal designado por éste, implementarán dichos controles. Se deberá considerar los siguientes lineamientos:

- Establecer una política formal prohibiendo el uso de software no-autorizado.
- Establecer una política formal para proteger contra riesgos asociados con la obtención de archivos, ya sea a través de redes externas o cualquier otro medio, indicando las medidas de protección a tomarse.
- La instalación y actualización regular de software para la detección o reparación de códigos maliciosos para revisar las computadoras y medios como un control preventivo o una medida rutinaria; los chequeos llevados a cabo debieran incluir:

a) Definición, gestión, procedimientos y responsabilidades para lidiar con la protección de códigos maliciosos en los sistemas, capacitación en su uso, reporte y recuperación de ataques de códigos maliciosos.
b) Preparar planes apropiados para la continuidad del negocio para recuperarse de ataques de códigos maliciosos, incluyendo toda la data y respaldo (back-up) de software y procesos de recuperación.
c) Implementar procedimiento para la recolección regular de información.

Actividades

- Establecer una política formal que prohíba el uso no autorizado de software.
- Establecer una política formal que proteja ante los riesgos asociados al obtener software y archivos a través de redes externas, o cualquier otro medio, indicando que medidas preventivas deber ser tomadas.
- Definir procedimientos y responsabilidades para tratar con código malicioso, entrenamiento en el uso, reporte recuperación ante ataques.
- Preparar apropiados planes de continuidad del negocio para recuperarse ante eventuales ataques.
- Implementar procedimientos para recopilar regularmente información como listas de correo o sitios informativos.

Dominio	**12**	**Seguridad en la Operativa**		
Objetivo de Control		Copias de seguridad.	**Control**	Copias de seguridad de la información.
12.3			**12.3.1**	

DESARROLLO

Propósito

Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Recomendación

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de
medios:
Se deben considerar los siguientes ítems para el respaldo de la información:

- Definir el nivel necesario de respaldo de la información.
- Producir registros exactos y completos de las copias de respaldo y procedimientos documentados de la restauración.
- La extensión (por ejemplo: respaldo completo o diferencial) y la frecuencia de los respaldos debiera reflejar los requerimientos comerciales de la organización, los requerimientos de seguridad de la información involucrada, y el grado crítico de la información para la operación continua de la organización.
- Las copias de respaldo se debieran almacenar en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el local principal.
- A la información de respaldo se le debiera dar el nivel de protección física y ambiental apropiado consistente con los estándares aplicados en el local principal; los controles aplicados a los medios en el local principal se debiera extender para

cubrir la ubicación de la copia de respaldo.

- Los medios de respaldo se debieran probar regularmente para asegurar que se puedan confiar en ellos para usarlos cuando sea necesaria en caso de emergencia.
- Los procedimientos de restauración se debieran chequear y probar regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación.
- En situaciones cuando la confidencialidad es de importancia, las copias de respaldo debieran ser protegidas por medios de una codificación.

Los procedimientos de respaldo de la plataforma debieran ser probados regularmente para asegurar que cumplan con los requerimientos de los planes de continuidad del negocio.

Actividades

- Proveer registros completos y registros de la información que se respalda, así también como los procedimientos de recuperación.
- Probar regularmente los medios de recuperación para asegurar que puedan ser utilizados.
- Los procedimientos de restauración deben ser probados regularmente.

Dominio	**12**	**Seguridad en la Operativa**		
Objetivo de Control		Registro de Actividad y Supervisión	**Control**	Registro y gestión de eventos de actividad.
12.4			**12.4.1**	

DESARROLLO

Propósito

Determinar el nivel de monitoreo requerido para implementar controles para la protección de los registros y gestión de eventos de actividad.

Recomendación

La plataforma debe ser monitoreada y protegida ante accesos no autorizados en las siguientes áreas

Acceso no autorizado

- ID del usuario.
- Fecha y hora de los eventos claves.
- Tipos de eventos.

Operaciones privilegiadas

- Uso de las cuentas privilegiadas.

Intentos de acceso no autorizados

- Accesos del usuario fallidas o rechazadas.
- Acciones fallidas o rechazadas que involucran la data y otros recursos.
- Alertas de los sistemas de detección de intrusiones.

Alertas o fallas del sistema

- Alertas o mensajes en la consola.
- Excepciones del registro del sistema..

Actividades

- Cumplir con los requerimientos legales relevantes aplicables para las actividades de monitoreo.
- Utilizar procedimientos de monitoreo para asegurar que los usuarios sólo estén realizando actividades para las cuales han sido explícitamente autorizados.

Dominio	**12**	**Seguridad en la Operativa**		
Objetivo de Control		Registro de Actividad y Supervisión	**Control**	Protección de los registros de información
12.4			**12.4.2**	

DESARROLLO

Propósito

Registrar y revisar periódicamente en particular las actividades de los administradores y operadores de sistema.

Recomendación

Los controles debieran tener el objetivo de proteger contra cambios no autorizados y problemas operacionales, y el medio de registro debiera incluir:

- Las alteraciones registradas a los tipos de mensajes.
- Los archivos de registro que se editan o borran.
- Capacidad de almacenamiento del medio de archivos de registro que se está excediendo, resultando en una falla en el registro de eventos o la escritura encima de los eventos registrados en el pasado.

Actividades

Los registros de administrador y operador del sistema debieran ser revisados de manera regular.

Dominio	**12**	**Seguridad en la Operativa**		
Objetivo de Control		Registro de Actividad y Supervisión	**Control**	Registros de actividad del administrador y operador del sistema
12.4			**12.4.3**	

DESARROLLO
Propósito Registrar las actividades del administrador de la plataforma y del administrador de servidores.
Recomendación Revisión periódica las actividades de los administradores y administrador de servidores. • Cuenta de administración u operación involucrada • Momento en el cual ocurre un evento, hora del evento. • Información acerca del evento. • Procesos involucrados.
Actividades • Los registros de administrador de la plataforma y administrador de servidores debieran ser revisados de manera regular. • Todas las cuentas con privilegios de usuario administrador o súper usuario deben ser continuamente registrados y monitoreadas.

Dominio	**12**	**Seguridad en la Operativa**		
Objetivo de Control		Registro de Actividad y Supervisión	**Control**	Sincronización de relojes
12.4			**12.4.4**	

DESARROLLO
Propósito Sincronizar con una fuente que proporcione la hora exacta los relojes de todos los sistemas involucrados con la plataforma Moodle de Apoyo a la Presencialidad.
Recomendación Se debiera utilizar un protocolo de hora de red para mantener todos los servidores sincronizados con el reloj maestro. Cuando una computadora o dispositivo de comunicaciones tiene la capacidad para operar un reloj de tiempo-real, este reloj debiera ser puesto a la hora de acuerdo a un estándar acordado; por ejemplo, el Tiempo Universal Coordinado (UTC) o la hora estándar local. Ya que algunos relojes se atrasan o adelantan a lo largo del tiempo, debiera existir un procedimiento que los revise y corrija cualquier variación significativa.
Actividades Se deben sincronizar los relojes de todos los sistemas críticos contra un reloj central, y éste a su vez sincronizado con un reloj en internet.

Dominio	12	Seguridad en la Operativa		
Objetivo de Control		Gestión de la vulnerabilidad técnica	**Control**	Gestión de vulnerabilidades técnicas
12.6			**12.6.1**	

DESARROLLO

Propósito

Obtener oportunamente la información sobre las vulnerabilidades técnicas de la plataforma Moodle de apoyo a la Presencialidad y las medidas apropiadas tomadas para tratar los riesgos asociados.

Recomendación

Se debiera tomar la acción apropiada y oportuna en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se debiera seguir el siguiente lineamiento para establecer un proceso de gestión efectivo para las vulnerabilidades técnicas:

- La organización debiera definir y establecer los roles y responsabilidades asociadas con la gestión de la vulnerabilidad técnica; incluyendo el monitoreo de la vulnerabilidad, evaluación del riesgo de la vulnerabilidad, monitoreo de activos y cualquier responsabilidad de coordinación requerida.
- Se debiera definir una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes.

Actividades

- Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia.

Dominio	12	Seguridad en la Operativa		
Objetivo de Control		Gestión de la vulnerabilidad técnica	**Control**	Restricciones en la instalación de software
12.6			**12.6.2**	

DESARROLLO

Propósito

Establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.

Recomendación

- Se deben establecer reglas que delimiten la instalación de nuevo software por parte de personal, solo debe contarse con el software necesario para el desarrollo de las funciones establecidas.

- Si no existen delimitaciones se incurre en el riesgo de que se instale en los equipos software que faciliten la intrusión de virus y código malicioso que atenta contra la seguridad de la información.

Actividades

- Definir normas de restricción en la instalación de nuevo software y dar a conocer al personal.

- Implementar programas que inhabiliten la instalación de software, como por ejemplo congeladores, estos garantizan que después de reiniciado el equipo se borren todos los programas instalados sin autorización.

- En caso de que surja la necesidad de implementar un nuevo software debe ser solicitado a la persona encargada.

Dominio	**12**	**Seguridad en la Operativa**		
Objetivo de Control		Consideraciones de las auditorías de los sistemas de información	**Control**	Controles de auditoría de los sistemas de información
12.7			**12.7.1**	

DESARROLLO

Propósito

Planificar y acordar cuidadosamente los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos y de la plataforma para minimizar el riesgo de interrupciones de los procesos.

Recomendación

a) Se deberían tener presente las siguientes lineamientos:

- Se debería acordar y controlar el alcance de las verificaciones.
- Los recursos para llevar a cabo las verificaciones se deberían identificar explícitamente estar disponibles.
- Todo acceso se debería monitorear y registrar para crear un rastro para referencia; el uso de rastros de referencia de tiempo se debería considerar.
- Se recomienda documentar todos los procedimientos, requisitos y responsabilidades.
- La persona que realiza la auditoría debería ser independiente de las actividades auditadas.

Actividades

- Acordar los requerimientos de auditoría con la autoridad.
- Acordar y controlar el alcance de los chequeos.
- Los chequeos deben limitarse a un acceso de "sólo lectura" a la plataforma.
- Identificar explícitamente y disponer los recursos para realizar los chequeos.
- Monitorear y registrar todos los accesos para producir un histórico de referencia.
- considerar rastros de referencia con impresión horaria para los datos o sistemas críticos.
- Documentar todos los procedimientos, requerimientos y responsabilidades.

Dominio	**13**	Seguridad en las telecomunicaciones		
Objetivo de Control		Gestión de la seguridad en las redes.	**Control**	Controles de red.
13.1			**13.1.1**	

DESARROLLO

Propósito

Manejar y controlar las redes con el fin de proteger la información en las redes, y mantener la seguridad de la plataforma y aplicaciones utilizando la red, incluyendo la información en tránsito.

Recomendación

El Responsable de administrar los servidores debiera implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados. En particular, se debieran considerar los siguientes ítems:

- Cuando sea apropiado, la responsabilidad operacional para las redes se debiera separar de las operaciones de cómputo.
- Se debieran establecer las responsabilidades y procedimientos para la gestión del equipo remoto, incluyendo el equipo en las áreas del usuario.
- Se debieran establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan a través de las redes públicas o a través de las redes inalámbricas; y proyectar los sistemas y aplicaciones conectados; también se pueden requerir controles especiales para mantener la disponibilidad de los servicios de la red y las computadoras conectadas.
- Se debiera aplicar registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes.
- Las actividades de gestión debieran estar estrechamente coordinadas para optimizar el servicio a la organización y para asegurar que los controles sean aplicados consistentemente a través de la infraestructura de procesamiento de la información.

Actividades

Separar la responsabilidad en la operación de las redes de las responsabilidades en el manejo de los servidores.

- Establecer responsabilidades y procedimientos de administración de equipamiento remoto.
- Establecer controles especiales para resguardar la confidencialidad e integridad de los datos que viajan sobre redes públicas o inalámbricas.
- Establecer los mecanismos apropiados de monitoreo y registro de las acciones relevantes para la seguridad.

Dominio	**13**	Seguridad en las telecomunicaciones	
Objetivo de Control	Gestión de la seguridad en las redes.	**Control**	Mecanismos de seguridad asociados a servicios en red.
13.1		**13.1.2**	

DESARROLLO

Propósito

Identificar e incluir las en el contrato de redes las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, ya sea que estos servicios sean provistos interna o externamente.

Recomendación

Los servicios de red incluyen la provisión de conexiones, servicios de redes privadas, redes de valor agregado y soluciones de seguridad de red manejadas como firewalls y sistemas de detección de intrusiones. Estos servicios pueden ir desde una simple banda ancha manejada ofertas complejas de valor agregado.

Las características de seguridad de los servicios de red pueden ser:

a. la tecnología aplicada para la seguridad de los servicios de red; como controles de autenticación, codificación y conexión de red.
b. cuando sea necesario, procedimientos para la utilización del servicio de red para restringir el acceso a los servicios de red o aplicaciones.

De acuerdo a lo anterior, se debiera determinar y monitorear regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura, y se debiera acordar el derecho de auditoría.

Actividades

- Aplicar tecnología para asegurar los servicios de red, tal como autenticación, encriptación y control de conexiones.
- Establecer conexiones seguras a través de reglas de accedo de acuerdo los requerimientos de la institución.

Dominio	**13**	Seguridad en las telecomunicaciones	
Objetivo de Control	Gestión de la seguridad en las redes.	**Control**	Segregación de redes.

13.1		**13.1.3**	

DESARROLLO

Propósito

Segregar los grupos de servicios de información, usuarios y sistemas de información en redes.

Recomendación

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "Gateway" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado.

Actividades

Crear "dominios de seguridad" en las redes de telecomunicaciones, pueden ser lógicos o físicos dependiendo de la tecnología implementada.

Dominio	**13**	Seguridad en las telecomunicaciones	
Objetivo de Control	Gestión de la seguridad en las redes.	**Control**	Políticas y procedimientos de intercambio de información.
13.2		**13.2.1**	

DESARROLLO

Propósito

Establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.

Recomendación

Diseñar los procedimientos y controles cuando se utilizan medios de comunicación electrónicos para el intercambio de información. Se debieran considerar los siguientes ítems:

- Los procedimientos diseñados para proteger el intercambio de información de la intercepción, copiado, modificación, routing equivocado y destrucción.
- Los procedimientos para la detección y protección de contra códigos maliciosos que pueden ser transmitidos a través del uso de comunicaciones electrónicas.
- Los procedimientos para el uso de comunicación inalámbrica, tomando en cuenta los riesgos particulares involucrados.
- Uso de técnicas de codificación; por ejemplo, para proteger la confidencialidad, integridad y autenticidad de la información.
- No dejar la información confidencial o crítica en medios impresos; por ejemplo, copiadoras, impresoras y máquinas de fax; ya que personal no-autorizado puede tener acceso a ellas.

- Recordar al personal que debiera tomar las precauciones apropiadas; por ejemplo, no revelar información confidencial cuando realiza una llamada telefónica para evitar ser escuchado o interceptado por:

a) Personas alrededor suyo, particularmente cuando se utilizan teléfonos Móviles.
b) Intervención de teléfonos y otras formas de escucha no-autorizada a través del acceso físico al teléfono o la línea telefónica, o el uso de escáneres receptores.
c) Personas en el otro lado de la línea, en el lado del receptor.

- Además, se debiera recordar al personal que no debieran mantener conversaciones confidenciales en lugares públicos, u oficinas o salas de reuniones abiertas, sin paredes a prueba de ruidos.

Actividades

Diseñar los procedimientos para proteger el intercambio de información de la intercepción, copiado, modificación y destrucción.

- Diseñar el procedimiento para la detección y protección en contra de códigos maliciosos que puedan ser trasmitidos a través del uso de comunicaciones electrónicas.
- Diseñar el procedimiento para proteger la información electrónica confidencial.
- Crear una política o lineamiento para el uso aceptable de los medios de comunicación electrónicos.
- Crear el procedimiento para el uso de comunicación inalámbrica, tomando en cuenta los riesgos particulares involucrados.

Dominio	**13**	Seguridad en las telecomunicaciones		
Objetivo de Control		Gestión de la seguridad en las redes.	**Control**	Mensajería electrónica.
13.2			**13.2.3**	

DESARROLLO

Propósito

Proteger adecuadamente la información involucrada en mensajes electrónicos.

Recomendación

Los mensajes electrónicos como el correo electrónico y los mensaje instantáneos representa un papel cada vez más importante en las comunicaciones comerciales. Los mensajes electrónicos tienen riesgos diferentes que las comunicaciones basadas en papel.
Las consideraciones de seguridad para los mensajes electrónicos debieran incluir lo siguiente:

- Proteger los mensajes del acceso no autorizado, modificación o negación del servicio.
- Asegurar la correcta dirección y transporte del mensaje. Confiabilidad y disponibilidad general del servicio.

Actividades

Proteger los mensajes del acceso no autorizado, modificación o negación del servicio.

- Asegurarla correcta asignación de la dirección y el transporte del mensaje.
- Niveles altos de controles de autenticación para los accesos desde las redes públicamente accesibles.

Dominio	**13**	Seguridad en las telecomunicaciones		
Objetivo de Control		Gestión de la seguridad en las redes.	**Control**	Acuerdos de confidencialidad y secreto.
13.2			**13.2.4**	

DESARROLLO

Propósito

Identificar y revisar regularmente que los requerimientos de confidencialidad o acuerdos de no divulgación reflejan las necesidades de la organización para proteger la información de la plataforma Moodle de apoyo a la presencialidad.

Recomendación

Se deberá definir, implementar y revisar regularmente los acuerdos de confidencialidad o de no divulgación para la protección de la información de la Universidad Francisco de Paula Santander Ocaña. Dichos acuerdos deberán responder a los requerimientos de confidencialidad o no divulgación de la información de la UFPSO; además, deberán ser revisados de acuerdo a la fecha estipulada en el control. Asimismo, deberá cumplir con toda legislación o normativa que alcance a la Universidad en materia de confidencialidad de la información.

Actividades

Clasificación de la información (pública/secreta).

- Definición de la duración del acuerdo, incluyendo la duración indefinida.
- Estipulación de las acciones necesarias una vez que el acuerdo haya terminado.
- Asignación de responsabilidades para evitar la divulgación no autorizada de la información.
- Describir las acciones necesarias en el caso de no cumplir con el acuerdo.

Dominio	**14**	Adquisición, desarrollo y mantenimiento de los sistemas de información		
Objetivo de Control		Requisitos de seguridad de los sistemas de información.	**Control**	Análisis y especificación de los requisitos de seguridad
14.1			**14.1.1**	

DESARROLLO

Propósito

Especificar los requisitos para los controles de seguridad sobre los requisitos del negocio para mejoras a la plataforma Moodle de Apoyo a la Presencialidad.

Recomendación
Los requerimientos para mejoras a la plataforma especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar a la plataforma, como así también controles manuales de apoyo.

Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados. Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto. Cuando se proporciona funcionalidad adicional y ello causa un riesgo de seguridad, tal funcionalidad se debería inhabilitar o se debería revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

Actividades

- Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.

Dominio	**14**	Adquisición, desarrollo y mantenimiento de los sistemas de información		
Objetivo de Control		Requisitos de seguridad de los sistemas de información.	**Control**	Seguridad de las comunicaciones en servicios accesibles por redes públicas
14.1			**14.1.2**	

DESARROLLO

Propósito
Manejar la Seguridad de las comunicaciones en servicios accesibles por redes públicas

Recomendación
El administrador de servidores debiera implementar controles para asegurar la información en las redes públicas en espacial establecer controles especiales para salvaguardar la confidencialidad y la integridad de la data que pasa a través de las redes públicas o a través de las redes inalámbricas.

Actividades
Establecer controles especiales para resguardar la confidencialidad e integridad de los datos que viajan sobre redes públicas o inalámbricas.

Dominio	**14**	Adquisición, desarrollo y mantenimiento de los sistemas de información		
Objetivo de Control		Seguridad en los procesos de desarrollo y soporte.	**Control**	Procedimientos de control de cambios en los sistemas
14.2			**14.2.2**	

DESARROLLO

Propósito
Controlar la implementación de los cambios mediante el uso de procedimientos formales para el control del cambio de la plataforma Moodle de apoyo a la presencialidad.

Recomendación
Se debieran documentar y hacer cumplir los procedimientos formales de control del cambio para minimizar la corrupción de la plataforma. Los cambios importantes a la plataforma debieran realizarse después de un proceso formal de documentación, especificación, prueba, control de calidad e implementación manejada.

Este proceso debiera incluir una evaluación del riesgo, análisis de los impactos del cambio y la especificación de los controles de seguridad necesarios. Este proceso también debiera asegurar que los procedimientos de seguridad y control existentes no se vean comprometidos.

Actividades
Mantener un registro de los niveles de autorización acordados.

- Asegurar que los cambios sean presentados por los usuarios autorizados.
- Revisar los procedimientos de control e integridad para asegurar que no se vean comprometidos por los cambios.
- Obtener la aprobación formal para propuestas detalladas antes de comenzar el trabajo.
- Asegurar que los usuarios autorizados acepten a los cambios antes de la implementación.
- Mantener un control de la versión para todas las actualizaciones de la plataforma.
- Asegurar que la documentación de operación y procedimientos de usuarios sean cambiados conforme sean necesarios para seguir siendo apropiados.

Dominio	**14**	Adquisición, desarrollo y mantenimiento de los sistemas de información		
Objetivo de Control		Seguridad en los procesos de desarrollo y soporte.	**Control**	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2			**14.2.3**	

DESARROLLO

Propósito
Revisar y probar la plataforma Moodle de apoyo a la presencialidad para asegurar que no exista un impacto adverso en la seguridad cuando se cambian los sistemas de operación.

Recomendación

- Revisar los procedimientos de control e integridad de la aplicación para asegurar que no se hayan visto comprometidos por los cambios en el sistema de operación.
- Asegurar que el plan y el presupuesto de soporte anual abarque las revisiones y pruebas del sistema resultantes de los cambios en el sistema de operación.
- Asegurar que la notificación de los cambios en el sistema de operación sea provista con tiempo para permitir realizar las pruebas y revisiones apropiadas antes de la implementación.

Actividades
Definir un procedimiento que incluya:

- Procedimientos de control e integridad de la aplicación.
- Proveer y notificar con tiempo los cambios en el sistema de operación.
- Realizar los cambios apropiados en los planes de continuidad del negocio.

Dominio	**14**	Adquisición, desarrollo y mantenimiento de los sistemas de información		
Objetivo de Control		Seguridad en los procesos de desarrollo y soporte.	**Control**	Restricciones a los cambios en los paquetes de software.
14.2			**14.2.4**	

DESARROLLO

Propósito
No fomentar modificaciones a la plataforma, se debieran limitar a los cambios necesarios y todos los cambios debieran ser estrictamente controlados.

Recomendación
Mientras sea posible y practicable, se debieran utilizar los paquetes de Moodle sin modificaciones. Cuando se necesita modificar, se debieran considerar los siguientes puntos:

- El riesgo de comprometer los controles incorporados y los procesos de integridad.
- El impacto de si como resultado de los cambios, la UFPSO se hace responsable del mantenimiento futuro de la plataforma.

Si son necesarios cambios, se debiera mantener la plataforma moodle original y se debieran aplicar los cambios en una copia claramente identificada. Todos los cambios debieran ser completamente probados y documentados, de manera que puedan ser replicados, si fuese necesario, a las futuras actualizaciones.

Dominio	**14**	Adquisición, desarrollo y mantenimiento de los sistemas de información		
Objetivo de Control		Seguridad en los procesos de desarrollo y soporte.	**Control**	Uso de principios de ingeniería en protección de sistemas.
14.2			**14.2.5**	

DESARROLLO

Propósito
Utilizar los principios de ingeniería en protección la Plataforma de Apoyo a la Presencialidad.

Recomendación
Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.

Dominio	**15**	Relaciones con suministradores		
Objetivo de Control		Gestión de la prestación del servicio por suministradores	**Control**	Supervisión y revisión de los servicios prestados por terceros.
15.2			**15.2.1**	
DESARROLLO				
Propósito Supervisar y revisar los servicios prestados por terceros.				
Recomendación Se recomienda realizar una supervisión y revisión al servicio prestado por terceros, en este caso, a moodle.org y las opciones que brinda para mantener en funcionamiento la Plataforma de Apoyo a la Presencialidad				

Dominio	**15**	Relaciones con suministradores		
Objetivo de Control		Gestión de la prestación del servicio por suministradores	**Control**	Gestión de cambios en los servicios prestados por terceros.
15.2			**15.2.2**	
DESARROLLO				
Propósito Gestionar los cambios que se realicen a través del servicio prestado por terceros.				
Recomendación La Plataforma de Apoyo a la Presencialidad al estar basada en Moodle, es necesario realizar cambios de versión a la más reciente, según las necesidades del sistema. Se recomienda analizar los cambios que han tenido las versiones y así determinar si es necesaria la actualización.				
Actividades • Revisar los cambios entre una versión actualmente utilizada y las nuevas.				

Dominio	**16**	Gestión de incidentes en la seguridad de la información		
Objetivo de Control		Gestión de incidentes en la seguridad de la información y mejoras	**Control**	Responsabilidades y procedimientos.
16.1			**16.1.1**	
DESARROLLO				
Propósito Establecer funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.				

Recomendación

Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo como mínimo:

- Fallas operativas
- Código malicioso
- Intrusiones
- Fraude informático
- Error humano
- Catástrofes naturales
- Definición de las primeras medidas a implementar
- Análisis e identificación de la causa del incidente.
- Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
- Comunicación formal con las personas afectadas o involucradas con la recuperación, del incidente.

Actividades

Establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados.

Dominio	**16**	Gestión de incidentes en la seguridad de la información		
Objetivo de Control		Gestión de incidentes en la seguridad de la información y mejoras	**Control**	Notificación de los eventos de seguridad de la información
16.1			**16.1.2**	

DESARROLLO

Propósito

Reportar los eventos de seguridad de la información a través de los canales apropiados lo más rápidamente posible.

Recomendación

Se debiera establecer un procedimiento formal para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de intensificación de incidentes, estableciendo la acción a tomarse al recibir un reporte de un evento en la seguridad de la información. Se debiera establecer un punto de contacto para el reporte de eventos en la seguridad de la información.

Se debiera asegurar que este punto de contacto sea conocido a través de toda la organización, que siempre esté disponible y sea capaz de proporcionar una respuesta adecuada y oportuna.

Todos los usuarios empleados, contratistas y terceros debieran estar al tanto de la responsabilidad de reportar cualquier evento en la seguridad de la información lo más rápidamente posible. También debieran estar al tanto del procedimiento para reportar eventos en la seguridad de la información y el punto de contacto. Los procedimientos de reporte debieran incluir:

Procesos de retroalimentación adecuados para asegurar que aquellos que reportan eventos en la seguridad de la información sean notificados de los resultados después de haber tratado y terminado con el problema.

- Formatos donde se reporte los eventos en la seguridad de la información para respaldar la acción de reporte, y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento en la seguridad de la información.
- Se debiera tomar la conducta correcta en el caso de un evento en la seguridad de la información; es decir, anotar todos los detalles importantes inmediatamente.

Actividades

- Establecer un procedimiento formal para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de notificación de incidentes, estableciendo la acción a tomarse al recibir un reporte de un evento en la seguridad de la información.
- Establecer un punto de contacto para el reporte de eventos en la seguridad de la información, dicho punto de contacto debe ser conocido por toda la Universidad; además, siempre deberá estar disponible.

Dominio	**16**	Gestión de incidentes en la seguridad de la información		
Objetivo de Control		Gestión de incidentes en la seguridad de la información y mejoras	**Control**	Notificación de puntos débiles de la seguridad.
16.1			**16.1.3**	

DESARROLLO

Propósito

Requerir que todos los usuarios empleados, contratistas y terceros tomen nota y reporten cualquier debilidad de seguridad observada o sospechada en la plataforma.

Recomendación

Todos los usuarios empleados, contratistas y terceros debieran reportar estos temas al administrador de la plataforma, lo más rápidamente posible para evitar incidentes en la seguridad de la información. El mecanismo de reporte debiera ser fácil, accesible y estar disponible lo más posible.

Los usuarios empleados, contratistas y terceros debieran ser advertidos de no tratar de probar las debilidades de seguridad sospechadas. La prueba de las debilidades podría ser interpretada como un mal uso potencial del sistema y también podría causar daños al sistema o servicio de información y resultar en la responsabilidad legal para la persona que realiza la prueba.

Actividades

Dar a conocer a los empleados, contratistas y terceros el proceso de notificación de puntos débiles de seguridad.

Dominio	**16**	Gestión de incidentes en la seguridad de la información

Objetivo de Control	Gestión de incidentes en la seguridad de la información y mejoras	Control	Valoración de eventos de seguridad de la información y toma de decisiones
16.1		16.1.4	

DESARROLLO

Propósito

Reportar los eventos de seguridad de la información lo más rápidamente posible.

Recomendación

Se debiera establecer un procedimiento formal para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de intensificación de incidentes, estableciendo la acción a tomarse al recibir un reporte de un evento en la seguridad de la información.

Se debiera establecer un punto de contacto para el reporte de eventos en la seguridad de la información.

Todos los usuarios empleados, contratistas y terceros debieran estar al tanto de la responsabilidad de reportar cualquier evento en la seguridad de la información lo más rápidamente posible. También debieran estar al tanto del procedimiento para reportar eventos en la seguridad de la información y el punto de contacto. Los procedimientos de reporte debieran incluir:

- Procesos de retroalimentación adecuados para asegurar que aquellos que reportan eventos en la seguridad de la información sean notificados de los resultados después de haber tratado y terminado con el problema.
- Formatos donde se reporte los eventos en la seguridad de la información para respaldar la acción de reporte, y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento en la seguridad de la información.
- Se debiera tomar la conducta correcta en el caso de un evento en la seguridad de la información; es decir:

1. Anotar todos los detalles importantes inmediatamente.
2. No llevar a cabo ninguna acción por cuenta propia, sino reportar inmediatamente al punto de contacto.

- Referencia a un proceso disciplinario formal establecido para tratar con los usuarios empleados, contratistas o terceros que cometen violaciones de seguridad.

Actividades

- Establecer un procedimiento formal para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de notificación de incidentes, estableciendo la acción a tomarse al recibir un reposte de un evento en la seguridad de la información.

Dominio	16	Gestión de incidentes en la seguridad de la información		
Objetivo de Control		Gestión de incidentes en la seguridad de la	Control	Respuesta a los incidentes de seguridad.

16.1	información y mejoras	**16.1.5**	

DESARROLLO

Propósito

Establecer respuesta ante incidentes de seguridad

Recomendación

- Se debe formar a todo el personal de la institución que vaya a utilizar la plataforma Moodle de apoyo a la Presencialidad, sobre las normas de utilización, medidas de seguridad definidas, las instrucciones para tratar los recursos, esta una forma de disminuir los errores y los malos usos de los recursos y correcto desempeño de sus funciones.
- Evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados.

Dominio	**16**	Gestión de incidentes en la seguridad de la información	
Objetivo de Control	Gestión de incidentes en la seguridad de la información y mejoras	**Control**	Aprendizaje de los incidentes de seguridad de la información.
16.1		**16.1.6**	

DESARROLLO

Propósito

Definir un procedimiento que permita documentar, cuantificar y monitorear los costos de los incidentes y anomalías.

Recomendación

Se debiera utilizar la información obtenida de la evaluación de los incidentes en la seguridad de la información para identificar los incidentes recurrentes o de alto impacto.

Actividades

Evaluar la información obtenida a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

Dominio	**16**	Gestión de incidentes en la seguridad de la información	
Objetivo de Control	Gestión de incidentes en la seguridad de la información y mejoras	**Control**	Recopilación de evidencias.
16.1		**16.1.7**	

DESARROLLO

Propósito

Recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en la jurisdicción relevante.

Recomendación

Se debieran desarrollar y seguir los procedimientos internos cuando se recolecta y presenta evidencia para propósitos de una acción disciplinaria manejada dentro de una organización.

En general, las reglas de evidencia debieran abarcar:

- Admisibilidad de la evidencia: si la evidencia se puede o no se puede utilizar en la corte.
- Peso de la evidencia: la calidad e integridad de la evidencia.

Actividades

Para los documentos en papel: el original se debiera mantener de manera segura con un registro de la persona quien encontró el documento, el lugar donde se encontró el documento, cuándo se encontró el documento y quién presenció el descubrimiento; cualquier investigación debiera asegurar que no se alteren o manipulen los originales.

- Para la información en medios de cómputo: se debieran realizar imágenes dobles o copias de cualquier medio e información en discos duros o en memoria para asegurar su disponibilidad; se debiera mantener un registro de todas las acciones realizadas durante el proceso de copiado y el proceso debiera ser atestiguado; el medio original y el registro.

Dominio	**17**	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio		
Objetivo de Control		Continuidad de la seguridad de la información.	**Control**	Planificación de la continuidad de la seguridad de la información.
17.1			**17.1.1**	

DESARROLLO

Propósito

Se mantendrá un plan de continuidad de las actividades de la Plataforma de apoyo a la Presencialidad, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Recomendación

Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.

- Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Organismo y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.
- Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de la dependencia o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.
- Redactar los procedimientos de recuperación que describan las acciones a

emprender para restablecer las operaciones normales de la dependencia Unidad de Educación Virtual.

- Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.
- Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.
- Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda.

Actividades

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo.

Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

Dominio	**17**	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio		
Objetivo de Control		Continuidad de la seguridad de la información.	**Control**	Implantación de la continuidad de la seguridad de la información
17.1			**17.1.2**	

DESARROLLO

Propósito

Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la plataforma dentro de la Unidad de Educación Virtual.

Recomendación

Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.

- Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
- Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
- Documentar los procedimientos y procesos acordados.
- Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.

Actividades

Restaurar los servicios de comunicación específicos a los clientes en una cantidad de tiempo aceptable.

Se debiera asegurar que las copias de los planes de continuidad del negocio estén actualizadas y protegidas con el mismo nivel de seguridad aplicado en el lugar principal.

Dominio	**17**	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio		
Objetivo de Control		Continuidad de la seguridad de la información.	**Control**	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.1			**17.1.3**	
DESARROLLO				
Propósito Verificar y revisar la evaluación de la continuidad de la seguridad de la información.				
Recomendación Se recomienda mantener una revisión de la continuidad de la seguridad de la información, referente a la Plataforma de Apoyo a la Presencialidad.				

Dominio	**17**	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio		
Objetivo de Control		Redundancias	**Control**	Disponibilidad de instalaciones para el procesamiento de la información.
17.2			**17.2.1**	
DESARROLLO				
Propósito Revisar la disponibilidad de las instalaciones para el procesamiento de la información referente a la Plataforma de Apoyo a la Presencialidad.				
Recomendación • Almacenar los equipos redundantes y la información de las copias de seguridad en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal. • Se debería desarrollar procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente				

Dominio	**18**	Cumplimiento		
Objetivo de Control		Cumplimiento de los requisitos legales y contractuales.	**Control**	Identificación de la legislación aplicable
18.1			**18.1.1**	
DESARROLLO				

Propósito
Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la Unidad de Educación Virtual y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
Garantizar que la plataforma Moodle de apoyo a la presencialidad cumpla con la política, normas y procedimientos de seguridad de la institución.

Recomendación
Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para la plataforma. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

Actividades
Definir y documentar los controles y responsabilidades individuales específicos para satisfacer estos requerimientos.

Dominio	**18**	Cumplimiento	
Objetivo de Control	Cumplimiento de los requisitos legales y contractuales.	**Control**	Derechos de propiedad intelectual (DPI).
18.1		**18.1.2**	

DESARROLLO

Propósito
Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual.

Recomendación
Se debe considerar lo siguiente:

- Una política de cumplimiento de los derechos de propiedad intelectual y publicación que defina el uso legal de los productos.
- Mantener el conocimiento de las políticas para proteger los derechos de propiedad intelectual y las medidas disciplinarias aplicables a su transgresión.
- Mantener un registro de los activos e identificar todos aquellos protegidos por el derecho de propiedad intelectual.
- Mantener prueba y evidencia de la propiedad de las licencias, discos originales, manuales, etc.
- Implementar controles para asegurar que no se exceda el número máximo de usuarios permitidos.
- Proporcionar una política para mantener las condiciones de licencias en forma adecuada.

Actividades

- Mantener los documentos que acrediten la propiedad de licencias.
- Comprobar que se instale solo software autorizado y productos bajo licencia.

Dominio	**18**	Cumplimiento		
Objetivo de Control		Cumplimiento de los requisitos legales y contractuales.	**Control**	Protección de los registros de la organización
18.1			**18.1.3**	
DESARROLLO				
Propósito Proteger los registros importantes contra perdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales.				
Recomendación Los registros críticos de la institución se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la institución.				
Actividades Realizar un inventario de información clave y los controles para la protección de los registros y la información contra pérdida, destrucción o falsificación.				

Dominio	**18**	Cumplimiento		
Objetivo de Control		Cumplimiento de los requisitos legales y contractuales.	**Control**	Protección de datos y privacidad de la información personal.
18.1			**18.1.4**	
DESARROLLO				
Propósito Asegurar la protección y privacidad de la información conforme lo requiera la legislación, regulaciones y, si fuesen aplicables, las cláusulas contractuales relevantes.				
Recomendación Todos los empleados deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. La institución debiera incluir un "Compromiso de Confidencialidad", el cual debe ser suscrito por todos los empleados y contratistas. La copia firmada del compromiso será retenida en forma segura por el por la institución. Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer publicar información a ninguna persona, salvo autorización previa y escrita del Responsable del Activo.				

Actividades
Desarrollar e implementar una política de protección y privacidad de los datos. Esta política debe ser comunicada a todas las personas involucradas en el procesamiento de información personal.

Dominio	**18**	Cumplimiento	
Objetivo de Control	Cumplimiento de los requisitos legales y contractuales.	**Control**	Regulación de los controles criptográficos.
18.1		**18.1.5**	

DESARROLLO

Propósito
Utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.

Recomendación
- Restricciones sobre la utilización de la codificación.
- Métodos obligatorios o discrecionales para que las autoridades de los países tengan acceso a información codificada para garantizar su confidencialidad.

Dominio	**18**	Cumplimiento	
Objetivo de Control	Revisiones de la seguridad de la información.	**Control**	Revisión independiente de la seguridad de la información.
18.2		**18.2.1**	

DESARROLLO

Propósito
La seguridad de la información debe ser revisada de una manera independiente a intervalos planeados o cuando ocurran cambios significativos en la implementación de la seguridad, esto se hace con el fin de manejar la seguridad de la información y su implementación.

Recomendación
- La revisión independiente es necesaria para asegurar la continua idoneidad, eficiencia y efectividad del enfoque de la organización para manejar la seguridad de la información.
- La revisión debiera incluir las oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el enfoque por seguridad, incluyendo políticas y objetivos de control.
- La revisión debe ser llevada a cabo por personas independientes al área de revisión.
- Las personas que llevan a cabo estas revisiones debieran tener la capacidad y experiencia apropiada.
- Los resultados de la revisión independiente se debieran registrar y reportar a la

gerencia que inició la revisión y deben mantener los registros.

- Se debe realizar una revisión de las actividades de implantación al menos una vez al año.

Actividades

Las revisiones deben incluir las oportunidades de evaluación de mejoras y las necesidades de cambios de enfoque en la seguridad, incluyendo políticas y objetivos de control.

Dominio	**18**	Cumplimiento		
Objetivo de Control		Revisiones de la seguridad de la información.	**Control**	Cumplimiento de las políticas y normas de seguridad.
18.2			**18.2.2**	

DESARROLLO

Propósito

Los jefes de áreas debieran asegurar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para asegurar el cumplimiento de las políticas y estándares de seguridad.

Recomendación

Los jefes de áreas deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuadas, las normas y cualquier otro requisita de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

- Determinar la causa del incumplimiento.
- Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.
- Determinar e implementar la acción correctiva apropiada.
- Revisar la acción correctiva que se ejecutó.

Actividades

Detectar algún incumplimiento y determinar las causas, evaluar la necesidad de acciones correctivas, implementarlas, revisar dicha acción mediante su registro e informarlo.

Dominio	**18**	Cumplimiento		
Objetivo de Control		Revisiones de la seguridad de la información.	**Control**	Comprobación del cumplimiento.
18.2			**18.2.3**	

DESARROLLO

Propósito

Verificar periódicamente la plataforma Moodle de apoyo a la Presencialidad, para determinar el cumplimiento con las normas de implementación de la seguridad.

Recomendación
Verificar periódicamente que la plataforma Moodle de apoyo a la presencialidad cumpla con la política, normas y procedimientos de seguridad. La verificación del cumplimiento debiera comprender pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados.
Actividades • Realizar manualmente el chequeo del cumplimiento técnico por un especialista experimentado y/o con la asistencia de herramientas automatizadas que generen un reporte técnico. • Planificar, documentar y repetir las pruebas de intrusión o evaluaciones de vulnerabilidad. • Realizar la verificación de cumplimiento técnico por personal competente y autorizado o bajo su supervisión.

En la guía de buenas prácticas de la plataforma Moodle de apoyo a la presencialidad se excluyeron algunos dominios al no estar directamente relacionados con el tema tratado, a continuación se detallan estos dominios.

Tabla 15 Objetivos de control que no aplican

DOMINIO	OBJETIVO DE CONTROL		OBSERVACIONES
Aspectos Organizativos de la seguridad de la información	***6.2 Dispositivos para la movilidad y teletrabajo***		
	6.2.2	Teletrabajo.	Toda la información se gestiona desde las oficinas de la dependencia de la Unidad de Educación Virtual y la División de Sistemas para el caso de los servidores, no se trabaja desde lugares remotos.
Seguridad física y ambiental	***11.1 Áreas seguras***		
	11.1.6	Áreas de acceso público carga y descarga	No se cuenta con áreas de carga y descarga, para este tipo de empresa este control no aplica.
	11.2 Seguridad de los equipos		
	11.2.5	Salida de activos fuera de las dependencias de la empresa.	Los procesos realizados para la gestión de la plataforma Moodle de apoyo a la presencialidad no requieren retirar información o software fuera de la dependencia.
	11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	Los procesos realizados para la gestión de la plataforma Moodle de apoyo a la presencialidad no requieren retirar los equipos fuera de la dependencia.
Seguridad en las telecomunicaciones	***13.2 Intercambio de información con partes externas.***		
	13.2.2	Acuerdos de intercambio.	No se trabaja para empresas externas, todos

			los productos generados son para uso único y de propiedad de la Universidad Francisco de Paula Santander Ocaña.
Adquisición, desarrollo y mantenimiento de los sistemas de información	***14.3 Datos de prueba***		
	14.3.1	Protección de los datos utilizados en pruebas	Las pruebas no se realizan con información relevante, siempre se utiliza información no confidencial.
Relaciones con suministradores	***15.1 Seguridad de la información en las relaciones con suministradores***		
	15.1.1	Política de seguridad de la información para suministradores.	No se contratan terceras personas para la gestión de la plataforma Moodle de apoyo a la presencialidad.
	15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	La contratación con proveedores de componentes de infraestructura de TI son responsabilidades ajenas a la dependencia.
	15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	

Fuente. Autores del proyecto

5. CONCLUSIONES

- Al analizar los aspectos administrativos asociados a la seguridad lógica y física de la información se concluye que no existe una política de seguridad que permita regirse bajo la misma, para garantizar la integridad de la información, también se desconoce un plan de contingencia por parte del personal involucrado que permita sobrellevar cualquier eventualidad que ponga en riesgo la seguridad de la información.

- Se identificaron las vulnerabilidades y amenazas asociadas a los riesgos más representativos de la plataforma Moodle de apoyo a la presencialidad, a través de la cual fue posible determinar aquellos que son más críticos y que por ende requieren prioridad en la aplicación de controles, de igual manera se determinaron aquellos valorados como medios y bajos; entre los riesgos más críticos se detectaron aquellos derivados de la inexistencia y por ende desconocimiento de la misma.

- Los procesos de la plataforma de apoyo a la presencialidad se llevan de una manera segura, con respecto a copias de seguridad y asignación de roles, sin embargo, se debe definir los permisos de cada rol de forma segura, igualmente, se evidenció que no existen procedimientos para el registro de cambios que se realizan a través de la plataforma.

- Se realizó una guía de buenas prácticas especificando los controles, propósito, recomendaciones y actividades a realizar, según los hallazgos obtenidos en toda la investigación.

6. RECOMENDACIONES

Se recomienda la creación de un comité de seguridad de la información a quienes se les asigne la responsabilidad de crear y supervisar las políticas internas para la dependencia de Unidad de Educación Virtual de la UFPSO.

Para la creación de normativas se recomienda la implementación de la norma ISO/IEC 27002 ya que esta proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

Poner en práctica la guía de buenas prácticas desarrollada en esta investigación, dado que en ella se proponen planes de acción para el tratamiento de riesgos y amenazas y se presentan controles para dar seguimiento y respuesta oportuna a los incidentes que comprometan la integridad, disponibilidad y confiabilidad de la información.

Reubicar las instalaciones de la dependencia a un lugar donde no haya tanto flujo de personal e implementar mecanismos de control de acceso, sobre todo para la estación de trabajo del administrador de la plataforma.

BIBLIOGRAFÍA

COOPER, Sthepen, PIOTROWSKI, Victor. An exploration of the current state of information assurance education. 2009.

FUNDACIÓN DE EDUCACIÓN SUPERIOR INSTITUCIÓN TECNOLÓGICA SAN JOSE. La construcción de una política pública para la educación virtual en Colombia. 2011

UNIVERSIDAD AGUSTINIANA. Política Institucional de Educación Virtual. [En línea]. 2011. Disponible en internet: http://virtual.uniagustiniana.edu.co/Politica_Educacion_Virtual_Uniagustiniana.pdf

CALDERÓN MÉNDEZ, Neftalí de Jesús. [En línea]. 2010. [Recuperado el día 16 de junio de 2015] Disponible en internet: http://biblioteca.usac.edu.gt/tesis/08/08_0307_CS.pdf

RUIZ FAUDÓN, Sergio Luis. Introducción a los sistemas de bases de datos.2001.

THOMPSON, Iván. Definición de Información. [En línea]. 2008. [Recuperado el día 16 de Junio de 2015] Disponible en internet: http://moodle2.unid.edu.mx/dts_cursos_mdl/pos/MD/MM/AM/01/Definicion_de_Informacion.pdf

FERNÁNDEZ, Vicenç. Desarrollo de sistemas de información: una metodología basada en el modelado. 2010

GALINDO, Celvin. Seguridad de la información. La firma electrónica avanzada y su certificación. 2014
UNIVERIDAD FRANCISCO GAVIDIA. [En línea]. 2010. Disponible en internet: http://ri.ufg.edu.sv/jspui/bitstream/11592/7273/3/658.022-T689g-Capitulo%20II.pdf

MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.2012

UNIVERSIDAD INTERNACIONAL DE VALENCIA. Las plataformas LMS. [En línea]. 2007. Disponible en internet: http://www.apega.org/attachments/article/1056/plataformas_lms.pdf

BURGO, Jorge, CAMPOS, Pedro. Modelo Para la Seguridad de la Información en TIC. [En línea]. 2008. Disponible en internet: http://ceur-ws.org/Vol-488/paper13.pdf

MOODLE.ORG. [En línea]. 2007. Disponible en internet: https://docs.moodle.org/all/es/Acerca_de_Moodle

BOARD BRIEFING ON IT. Governance Institute. [En línea]. 2003. Disponible en internet: http://www.oecd.org/site/ictworkshops/year/2006/37599342.pdf

ALCALDÍA DE BOGOTÁ. [En línea]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

ALCALDÍA DE BOGOTÁ. [En línea]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

UNIVERSIDAD CATÓLICA. Tipos de Investigación según Grado de Profundidad y Complejidad. En línea]. 2012. [Recuperado el día 16 de junio de 2015] Disponible en internet: http://portalweb.ucatolica.edu.co/easyWeb2/files/17_6912_tipos-de-investigacian-.pdf

UNIVERSIDAD AUTÓNOMA DEL ESTADO HIDAGO. Aplicación básica de los métodos científicos. En línea]. 2012. [Recuperado el día 26 de Septiembre de 2015] Disponible en internet: http://www.uaeh.edu.mx/docencia/VI_Presentaciones/licenciatura_en_mercadotecnia/fundamentos_de_metodologia_investigacion/PRES39.pdf

ANEXOS

Anexo A Entrevista dirigida a la coordinadora de la Unidad de Educación Virtual

Universidad Francisco de Paula Santander
Facultad de Ingenierías
Especialización en Auditoría de Sistemas

Buenos días, como parte de nuestra tesis para la especialización en Auditoria de Sistemas de la Universidad Francisco de Paula Santander Ocaña, estamos realizando una investigación acerca de la gestión de la plataforma Moodle de apoyo a la presencialidad implementada en la Unidad de Educación Virtual. La información brindada en esta entrevista es de carácter confidencial, solo será utilizada con propósitos de esta investigación. Agradecemos enormemente su colaboración.

NOMBRE Y APELLIDOS **Yegny Karina Amaya Torrado**
NUMERO DE CÉDULA _____ TELEFONO_____
E-MAIL _____ FECHA: _____ _____ _____

Dominio 5: Política de Seguridad
¿Existe una política de seguridad de la información para la unidad, a través de la cual oriente una gestión segura de la plataforma?
¿El personal conoce y aplica la política de seguridad?
¿La política de seguridad es revisada periódicamente y actualizada?
Dominio 6: Aspectos Organizativos de la seguridad de la información
¿Cómo se distribuye la responsabilidad en cuanto al manejo de la información? a) Solo el administrador tiene acceso b) Existen varios tipos de usuario cada uno tiene asignados funciones específicas. c) Existen varios usuarios pero todos tiene los mismo privilegios
Dominio 7: Seguridad ligada a los recursos humanos
¿Qué criterios establece para saber que el personal que se va a contratar es el idóneo?
El personal de la unidad en el momento de ingresar a formar parte del equipo de trabajo ¿firman algún acuerdo de confidencialidad o de no divulgación, respecto del tratamiento de la información?
¿Se encuentran documentadas las funciones que le corresponden a cada una de los integrantes de la Unidad Virtual?
¿Con que regularidad se capacita al personal en cuanto a la gestión segura de la plataforma?
¿Existe algún proceso disciplinario en caso de que uno de los funcionarios atente contra la integridad de la información?
Cuando un funcionario deja de trabajar para la dependencia ¿Qué medidas de seguridad se toman respecto a la seguridad de la información?

Dominio 8: Gestión de Activos
¿Se cuenta con un inventario de activos en la unidad?
¿Existen responsabilidades asignadas respecto a la manipulación de activos de soporte físico en tránsito (ej: Discos duros externos)?
Dominio 9: Control de accesos
¿Se mantiene un proceso de autorización y un registro de todos los privilegios asignados?
¿Se cancelan inmediatamente los derechos de acceso de los usuarios que Cambiaron sus tareas o se desvinculan?
¿Existen diferentes niveles de privilegios de usuario?
¿Los equipos cuentan con contraseña de inicio de sesión?
Las contraseñas implementadas por los funcionarios de la unidad ¿se rigen por algún parámetro de contraseñas seguras?
Dominio 11: Seguridad física y ambiental
¿Considera adecuada la ubicación de las instalaciones físicas?
¿Existen controles para asegurar que el equipamiento, la información y el software no sean retirados de la dependencia sin autorización?
¿Existen controles para asegurar que personal no autorizado acceda a la dependencia?
¿Existe un plan de contingencia en caso de presentarse una catástrofe natural tanto para el personal, como para el recuperado de la información?
¿Qué tipo de mantenimiento se realiza a los equipos? ¿Con que frecuencia?
¿Existen normas para el puesto de trabajo despejado?
Dominio 12: Seguridad Operativa
¿Qué controles se llevan a cabo en cuanto al código malicioso?
¿Con que frecuencia se realizan las copias de seguridad?
¿Dónde se almacenan las copias de seguridad?
¿Existen bitácora de registros de cambios en la plataforma?
¿Existe la restricción para instalación de software?
¿Qué medidas/políticas de restricción del uso indebido de Internet existen en la dependencia?
Dominio 15: Relaciones con suministradores
¿La unidad contrata servicios con terceros?
¿Quién supervisa los servicios prestados por terceros?
Dominio 16: Gestión de incidentes en la seguridad de la información
Cuando ocurre un incidente, ¿Se recopilan las evidencias y se asignan responsabilidades para documentarlas a fin de aprender de dichos incidentes y monitorearlos?
Al detectar un evento de seguridad de la información, ¿Se registra, califica, prioriza y resuelve el incidente y se notifica a los usuarios afectados?
Dominio 17: Aspectos de seguridad de la información en la gestión de la continuidad del negocio
¿Se ha elaborado y documentado una estrategia de continuidad de las actividades de la dependencia consecuente con los objetivos?

Dominio 18: Cumplimiento
¿Se verifica que la plataforma cumpla con las políticas, normas, y procedimientos de seguridad establecidas? ¿De qué manera?
¿Están definidos y documentados claramente todos los requisitos legales, normativos y contractuales presentes para la plataforma de apoyo a la presencialidad?
¿Se realizan acciones para lograr la concienciación del personal respecto de las políticas de adquisición y derecho de propiedad intelectual sobre la adquisición del software?

Anexo B Lista de chequeo dirigida a la administradora de plataforma

Unidad de Educación Virtual			**R/PT: 001**	
CheckList			**C01**	
Dominio			**5. Políticas de seguridad**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
Al ser la información el activo más importante para la organización ¿están definidos los recursos de información que deben ser protegidos dentro de la Plataforma de Apoyo a la Presencialidad?				
¿Incluye un esquema de clasificación que preserve los criterios de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información contenida en la Plataforma de Apoyo a la Presencialidad?				
¿La Política de Seguridad de la Información implementada incluye normas y/o procedimientos para garantizar la continuidad de la plataforma, minimizando los riesgos de daño y asegurando el eficiente cumplimiento de los objetivos?				
¿Está sustentada la Política por una evaluación de riesgos?				
¿Contempla la Política las disposiciones legales vigentes?				
¿Existe una adecuada segregación de funciones para el administrador de la plataforma?				
¿Establece el resguardo adecuado de la información documentada?				
¿Establece la existencia de controles de acceso a la plataforma?				
¿Establece procedimientos de copias de seguridad de la información?				
¿Cuenta con control de acceso físico a sus instalaciones?				
Unidad de Educación Virtual			**R/PT: 002**	
CheckList			**C02**	
Dominio			**6. Aspectos organizativos de la seguridad de la información**	
Cuestionario				

Pregunta	SI	NO	NA	Comentarios
¿Existe un Responsable de Seguridad Informática designado por la máxima autoridad de la organización?				
¿Se encuentran definidos correctamente los procesos de seguridad de la información?				
¿Se ha realizado y documentado una evaluación de riesgo de la información de la Unidad?				
Unidad de Educación Virtual			**R/PT: 003**	
CheckList			**C03**	
Dominio			**7. Seguridad ligada a los recursos humanos**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se llevan a cabo controles de verificación (investigación de antecedentes) del personal en el momento en que se solicita el puesto?				
Quienes se incorporan a la organización ¿firman un acuerdo de confidencialidad o de no divulgación, respecto del tratamiento de la información de la plataforma?				
¿Es retenida por el Área de Recursos Humanos otra área competente, en forma segura la copia del acuerdo de confidencialidad suscripto por el personal, cualquiera sea su situación de revista?				
¿Se comunican en forma detallada al empleado las actividades que van a ser monitoreadas por el acuerdo?				
¿Se planifica la revisión del contenido del acuerdo de confidencialidad o de no divulgación a un plazo inferior a un año?				
¿Se determina la responsabilidad del empleado en materia de seguridad de la información, en los términos y condiciones del empleo?				
¿Se encuentran aclarados en los términos y condiciones de empleo, los derechos y obligaciones del empleado relativos a la seguridad de la información?				
¿Existen casos en los que las responsabilidades exceden la competencia del de la Unidad el horario normal de trabajo?				

¿Reciben los empleados de la Unidad una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la Unidad?				
¿Se tiene una política de inducción al personal antes de otorgar privilegios de acceso a los sistemas que corresponden?				
¿Se tiene un proceso formalizado para la terminación del contrato donde se incluya la devolución de contraseñas e información así como el equipo entregado previamente?				
¿Existen procedimientos para comunicar anomalías en la plataforma?				
¿Se cuenta con un proceso que documente, cuantifique y monitoree los tipos, volúmenes y costos de los incidentes y anomalías?				
¿Existe un canal de comunicación formalmente establecido para informar y dar respuesta a incidentes indicando la acción que ha de emprenderse?				
Unidad de Educación Virtual			**R/PT: 004**	
CheckList			**C04**	
Dominio			**8. Gestión de activos**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se encuentran completamente identificados y clasificados los activos importantes asociados a cada sistema de información en función de la administración de riesgos potenciales?				
¿Se elaboró un inventario con la información recabada sobre activos importantes? ¿Está actualizado?				
En la clasificación de los activos de información ¿se evalúan las tres (3) características sobre las que se basa la seguridad: confidencialidad, integridad y disponibilidad?				
¿Se realiza periódicamente un mantenimiento preventivo y prueba de los dispositivos de seguridad para la prevención, detección y extinción del fuego?				
Unidad de Educación Virtual			**R/PT: 005**	
CheckList			**C05**	

Dominio			9. Control de accesos	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Existen políticas, normas y procedimientos para Control de Acceso a la plataforma?				
¿Existen reglas de control de acceso obligatorias? Indicar en comentarios cuál es el criterio.				
¿Se promueve el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios?				
¿Los usuarios dan acuse de recibo de la recepción de la contraseña de carácter provisorio?				
Las contraseñas provisorias asignadas cuando los usuarios olvidan su contraseña se suministran sólo una vez identificado el usuario?				
Los sistemas operativos de red ¿están configurados de manera tal que las contraseñas tengan hasta ocho caracteres para cuentas administradoras y hasta seis caracteres para cuentas de usuarios comunes?				
¿Se suspende o bloquea permanentemente al usuario luego de tres (3) intentos de ingresar una contraseña incorrecta, siendo responsabilidad del usuario solicitar su rehabilitación?				
¿Se solicita a los usuarios el cambio de la contraseña cada 30 días?				
¿Se impide el uso de las últimas doce 12 contraseñas utilizadas?				
¿Se toman los recaudos necesarios a fin de garantizar que los usuarios cambien en su primer ingreso al sistema las contraseñas iniciales que les son asignadas?				
En dicho proceso ¿se revisan los derechos de acceso de los usuarios a intervalos no mayores de seis (6) meses o después de cualquier cambio?				
¿Se revisan las autorizaciones de privilegios especiales de derechos de acceso a intervalos no mayores de tres (3) meses?				
A fin de garantizar que no se obtengan				

privilegios no autorizados ¿se revisan las asignaciones de privilegios de todos los usuarios a intervalos no mayores de seis (6) meses?				
¿Garantizan los usuarios que los equipos desatendidos sean protegidos adecuadamente contra accesos no autorizados?				
¿Concluyen los usuarios las sesiones activas al finalizar las tareas o bien se protegen mediante un mecanismo de bloqueo adecuado?				
¿Existen procedimientos para la activación y desactivación del derecho de acceso a redes?				
¿Están identificadas las redes y servicios de red a los cuales se permite el acceso mediante normas y procedimientos?				
¿Existen gateways/firewalls en la Unidad que direccionen los puertos específicos a su correspondiente aplicación y a la vez descarten los paquetes con puertos de destino que no estén específicamente direccionados?				
¿Están divididos los grupos de usuarios de la Unidad en redes privadas virtuales o dominios lógicos?				
¿Se restringe el acceso a redes estableciendo dominios lógicos separados en redes virtuales separadas?				
¿Existen procedimientos que los usuarios deben seguir para solicitar el acceso a Internet en el caso de existir políticas de restricción para su utilización?				
¿Existen dispositivos de hardware o software utilizados para el monitoreo del uso de Internet?				
¿Existe en la Unidad, documentación en la que figuren las pautas de propiedades de seguridad de los servicios de red?				
¿Se limitan los horarios de conexión al horario normal de oficina?				
¿Se realizan informes sobre las actividades y el uso de la plataforma?¿Con qué frecuencia?				
Sobre las sesiones usuario ¿se establecieron controles de caducidad, tiempos de espera, etc.?				

¿Se han contemplado los sistemas críticos en las políticas de seguridad?				
¿Se monitorean accesos no autorizados?				
¿Se incluyen los detalles de identificación de usuario?				
¿Se registran fecha hora de eventos clave?				
¿Se distinguen tipos de eventos?				
¿Se observan los archivos a los que se accede?				
¿Se monitorean todas las operaciones que requieren privilegios especiales?				
¿Se monitorea el inicio y cierre del sistema?				
¿Se monitorea la conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos?				
¿Se monitorea el cambio de fecha/hora?				
¿Se monitorean los cambios en la configuración de la seguridad?				
¿Se monitorean intentos de accesos no autorizados como intentos fallidos?				
¿Se monitorean violaciones de la Política de Accesos y notificaciones para Gateway de red y firewalls?				
¿Existen alertas de sistema de detección de intrusiones?				
¿Existen alertas o mensajes de consola?				
¿Existen alarmas del sistema de administración de redes?				
¿Existen alarmas de accesos remotos al sistema?				
¿Los equipos que generan registros tienen correctamente configurados los relojes?				
Unidad de Educación Virtual			**R/PT: 006**	
CheckList			**C06**	
Dominio			**10. Cifrado**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se ha implementado un sistema de administración de claves criptográficas?				
¿Utiliza la Unidad técnicas criptográficas de clave pública y clave privada?				
¿Se protegen las claves contra la modificación y/o destrucción, copia o divulgación?				

¿Se protege el equipamiento destinado a generar, almacenar y archivar claves?				
¿Se han redactado normas, procedimientos y métodos de administración de claves para generar, almacenar, actualizar, revocar, recuperar, archivar y destruir las mismas?				
¿Tienen las claves fechas de entrada caducidad de vigencia?				
¿Se cuenta con certificados de clave pública?				
¿Existen normas o procedimientos para proteger los datos de prueba del sistema?				
Unidad de Educación Virtual			**R/PT: 007**	
CheckList			**C07**	
Dominio			**11. Seguridad Física y Ambiental**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Establece la Política, en forma clara y sencilla, sus objetivos y alcances generales?				
¿Incluye mínimamente los tópicos de organización de la seguridad, clasificación y control de activos, seguridad del personal, seguridad física y ambiental, gestión de comunicaciones y las operaciones, control de acceso, desarrollo y mantenimiento de los sistemas, administración de la continuidad de las actividades cumplimiento, entre otros?				
Al ser la información un activo para la organización ¿están definidos los recursos de información que deben ser protegidos?				
¿Incluye un esquema de clasificación que preserve los criterios de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad?				
¿La Política de Seguridad de la Información implementada incluye normas y/o procedimientos para garantizar la continuidad de los sistemas de información, minimizando los riesgos de daño y asegurando el eficiente cumplimiento de los objetivos de la Unidad?				
¿Está sustentada la Política por una evaluación de riesgos?				
¿Es la Política concordante con los objetivos de la Unidad?				

¿Contempla la Política las disposiciones legales vigentes?				
¿Define las responsabilidades de las personas, departamentos y organizaciones para los que aplica la política de seguridad?				
¿Define los roles objetivos para cada nivel de responsabilidad?				
¿Existe una adecuada segregación de funciones dentro del área de sistemas?				
¿Define las sanciones en caso de incumplimiento?				
¿Establece el resguardo adecuado de la información documentada?				
¿Establece la existencia de controles de acceso a la información?				
¿Establece la existencia de procedimientos de copias de seguridad de la información?				
¿Se lleva a cabo la asignación de responsabilidades de la seguridad informática?				
¿Resguarda todos los procesos vinculados a la Unidad?				
¿Define la Política sanciones ante casos de incumplimientos?				
¿Cuenta el centro de cómputos con sistemas de control de acceso físico a sus instalaciones?				
¿Cumple el personal del Área de Sistemas con el perfil adecuado para el cargo que desempeña?				
Unidad de Educación Virtual			**R/PT: 008**	
CheckList			**C08**	
Dominio			**12. Seguridad en la Operativa**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se controlan los cambios en los sistemas y en los recursos de tratamiento de la información?				
Se gestionan los cambios en la provisión del servicio y en los procedimientos y los controles se tiene en cuenta la importancia de los sistemas y procesos de la Unidad de Educación Virtual.				
¿Los cambios propuestos tienen la				

autorización de los usuarios y/o del propietario de la información?				
¿Pueden los cambios comprometer la integridad de los controles y procedimientos?				
¿Están definidos los procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento?				
¿Se documenta la gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones?				
¿Se han desarrollado procedimientos vinculados a la concienciación de los usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios?				

Unidad de Educación Virtual	**R/PT: 009**
CheckList	**C09**
Dominio	**13. Seguridad en las Telecomunicaciones**

Cuestionario

Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se documenta y se mantienen los procedimientos de operación y se ponen a disposición de todos los usuarios que lo necesiten?				
¿Se tiene separadas las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la Unidad de Educación Virtual?				
¿Tiene separado los recursos para el desarrollo, prueba y producción?				
¿La organización verifica la implementación de acuerdos con terceros?				
¿Los servicios, informes y registros suministrados por terceros son monitoreados y revisados regularmente?				
¿Se realiza proyecciones de los requisitos de capacidad a futuro para reducir el riesgo de sobrecarga de los sistemas?				
¿Se documenta y se prueba, antes de su aceptación, los requisitos operacionales de los nuevos sistemas?				

Se desarrollan las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación?				
Se tiene implementado controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios?				
Se cuenta con ciertas precauciones para prevenir y detectar la introducción de código malicioso no autorizado?				
Los administradores introducen controles y medidas especiales para detectar o evitar la introducción de software malicioso o no autorizado?				
Se tiene establecido procedimientos de respaldo para realizar copias de seguridad y probar su puntual recuperación?				
Se realiza regularmente copias de seguridad de toda la información como cursos y de la plataforma?				
Tiene establecido el tipo de almacenamiento, frecuencia de copia y prueba de soportes y lugar de respaldo?				
Se controla adecuadamente las redes para protegerlas de amenazas?				
Se mantiene la seguridad en los sistemas y aplicaciones que utilizan las redes?				
Tiene implantado estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red?				
Tiene establecido procedimientos para la gestión de los medios informáticos removibles?				
Se protege la documentación de los sistemas contra accesos no autorizados?				
Tiene establecido los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción?				
Se protegen los medios que contienen				

información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la dependencia?				
Tiene establecido los procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito?				
Los sistemas se monitorean y los eventos de la seguridad de información son registrados?				
Se registran las actividades del administrador y de los operadores del sistema?				
Se registran, analizan y toman acciones apropiadas de las averías?				
Se produce y se mantiene durante un periodo establecido los registros de auditoría con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información, con el fin de facilitar las investigaciones futuras y el monitoreo?				
Unidad de Educación Virtual			**R/PT: 010**	
CheckList			**C10**	
Dominio			**14. Adquisición, desarrollo y mantenimiento**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se han planificado, documentado y ejecutado los requerimientos de seguridad de las etapas de Desarrollo, Implementación y Mantenimiento del sistema?				
¿Existen registros de auditoría que controlen la validación de los datos de entrada, salida y procesamiento interno?				
¿Se han incorporado reglas de validación de campos en los programas o formularios de entrada de datos o en la definición de las tablas de la base de datos?				
¿Se ha implementado un formulario de solicitud de modificación de programas una hoja de seguimiento de los casos de la modificación?				
¿Se impide que el administrador tenga permisos de modificación sobre los programas fuentes bajo su custodia?				
¿Existe un responsable único para cada				

aplicación desarrollada internamente o adquirida a un proveedor externo? ¿Fue designado formalmente?				
¿Se mantiene un control de versiones para todas las actualizaciones de la plataforma?				
¿Se garantiza que la implementación se llevará a cabo minimizando la discontinuidad de las actividades?				
¿Se dispone de herramientas preventivas para evitar la infección de la plataforma con código malicioso?				
Unidad de Educación Virtual			**R/PT: 011**	
CheckList			**C11**	
Dominio			**15. Relaciones con suministradores**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
Es conocida la política de seguridad de la información para suministradores?				
Se cuenta con un tratamiento del riesgo dentro de acuerdos de suministradores?				
Se tiene en cuenta una cadena de suministro en tecnologías de la información y Comunicaciones?				
Se realiza una supervisión y revisión de los servicios prestados por terceros?				
Se realiza una gestión de cambios en los servicios prestados por terceros?				
Unidad de Educación Virtual			**R/PT: 012**	
CheckList			**C12**	
Dominio			**16. Gestión de incidentes en la seguridad de la información**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se establecen responsabilidades y procedimientos de manejo de incidentes?				
¿Existen procedimientos para los planes de contingencia normales ante eventuales incidentes?				
¿Se documentan en forma detallada todas las acciones de emergencia adoptadas?				
¿Se notificó de la medida adoptada ante la contingencia a la autoridad y/o organismos pertinentes?				

¿Se contemplan los incidentes relativos a la seguridad ocasionados por fallas operativas?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por código malicioso?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por intrusiones?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por fraude informático?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por error humano?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por catástrofes naturales?				
¿Se analizó el incidente y se identificó su causa?				
¿Se planificaron e implementaron las soluciones a efectos de evitar la repetición del incidente?				
¿Se comunican las acciones de emergencia al jefe inmediato? ¿Se revisa su cumplimiento?				
Unidad de Educación Virtual			**R/PT: 013**	
CheckList			**C13**	
Dominio			**17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
Existe un Comité de Seguridad de la Información el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de la actividad de la Unidad?				
¿Se han definido objetivos organizacionales de las herramientas de procesamiento de información?				
¿Está la administración de la continuidad de las actividades de la Unidad incorporada a los procesos y estructura del mismo?				
¿Se han identificado y priorizado los procesos críticos de las actividades de la Unidad?				
¿Comprenden los integrantes de la Unidad los riesgos que el mismo enfrenta, en términos de probabilidades de ocurrencia e impacto de las				

posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del organismo?				
¿Se ha elaborado y documentado una estrategia de continuidad de las actividades de la Unidad consecuente con los objetivos y prioridades acordadas?				
¿Se han aprobado planes de continuidad de las actividades de la Unidad de conformidad con la estrategia de continuidad acordada?				
¿Se han coordinado pruebas y actualizaciones periódicas de los planes y procesos implementados?				
¿Se ha considerado la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la Unidad?				
¿Se han identificado los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades como por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio?				
¿Se han evaluado los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación?				
¿Se identificaron los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y se especificaron las prioridades de recuperación?				
¿Se han identificado los controles preventivos (sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc)?				
¿Han participado los propietarios de los procesos y recursos de información y el Responsable de Seguridad Informática en el proceso de identificación y evaluación de riesgos?				
¿Se consideraron todos los procesos de las actividades de la Unidad sin Imitarse a las				

instalaciones de procesamiento de la información?				
Como resultado de la evaluación de riesgos ¿se ha desarrollado un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la Unidad?				
¿El plan estratégico ha sido aprobado por el Comité de Seguridad de la Información?				
Dicho Comité ¿ha elevado el Plan Estratégico a la máxima autoridad de la organización para su aprobación?				
¿Se documentaron los procedimientos y procesos de emergencia acordados?				
¿Se llevó a cabo la capacitación adecuada del personal en materia de procedimientos procesos de emergencia incluyendo el maneo de crisis?				
¿Se desarrolló el proceso de capacitación del personal involucrado en los procedimientos de reanudación y recuperación?				
¿Se trataron mecanismos de coordinación y comunicación entre equipos (personal involucrado)?				
¿Se incluyeron procedimientos de divulgación en el plan de contingencia?				
¿Se contemplaron requisitos en materia de seguridad?				
¿Se adecuaron procesos específicos para el personal involucrado?				
¿Cuenta el personal involucrado con documentación específica que indique cuál es su participación en el proceso de contingencia?				
¿Se designó a los responsables de ejecutar cada componente del mismo?				
¿Se encuentran definidos los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones de la Unidad y/o la vida humana?				
¿Existen procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de la				

Unidad o de servicios de soporte a ubicaciones transitorias alternativas?				
¿Se redactaron los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la Unidad?				
¿Se definió un cronograma de mantenimiento que especifique cómo y cuándo se probará el plan, y el proceso para el mantenimiento del mismo?				
¿Se realizaron actividades de concientización y capacitación diseñadas para propiciar la comprensión de los procesos de continuidad del negocio y garantizar que los procesos sigan siendo eficaces?				
¿Se realizaron simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión luego de incidentes o crisis)?				
¿Se revisan y actualizan periódicamente los planes de continuidad de las actividades de la Unidad para garantizar su eficacia permanente?				
¿Existe un programa de administración de cambios de la Unidad que incluya procedimientos para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades?				
Unidad de Educación Virtual			**R/PT: 014**	
CheckList			**C14**	
Dominio			**18. Cumplimiento**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Incluyen estas normas de procedimiento controles específicos y responsabilidades individuales que garanticen el cumplimiento de los recursos de tecnología informática?				
¿Se verifica que los sistemas de información cumplan con las políticas, normas, y procedimientos de seguridad establecidas?				
¿Se solícita, en caso de ser necesario, la participación de especialistas externos?				
El funcionario a cargo del Área Legal con la asistencia del Responsable de la Seguridad				

Informática ¿definió y documentaron todos los requisitos legales, normativos y contractuales que debe cumplir cada uno de los sistemas de información?				
El funcionario a cargo del Área Legal con la asistencia del Responsable de la Seguridad Informática ¿redactó un Acuerdo de Confidencialidad para ser suscripto por todos los integrantes de la organización?				
¿Existe una fi gura sobre la cual recae la responsabilidad de hacer cumplir las normas y procedimientos de seguridad?				
¿Se han implementado procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por las normas de propiedad intelectual?				
¿Utilizan los empleados únicamente material autorizado por la Unidad?				
¿Se respetan las normas que fijan los derechos de propiedad intelectual de los sistemas de información, procedimientos, documenta?				

Fuente. Autores del proyecto

Anexo C Encuesta dirigida al personal de la División de Sistemas

Dirigida a: Personal de la División de Sistemas cuya labor se relacionan con el manejo de la plataforma Moodle, actualizaciones y servidores donde se encuentra alojada dicha plataforma.

Objetivo: Esta encuesta tiene como objetivo recopilar información que nos permita realizar un análisis sobre la gestión de la plataforma Moodle implementada en la Unidad de Educación Virtual de la Universidad Francisco de Paula Santander Ocaña (UFPSO).
La información que usted nos suministre será muy importante para la investigación y será utilizada con toda reserva por los investigadores.
Esta encuesta está compuesta en su mayoría por preguntas cerradas con varias opciones de respuesta, por favor marque con una X la respuesta que considere apropiada según su criterio.

1. ¿Existen políticas de seguridad de la información?

SI____NO _____ NS/NC_____

2. ¿Conoce y entiende la política de seguridad, su propósito e implicaciones?

SI___NO___

3. ¿A través de qué medios se le dio a conocer la política?

Inducción___ Circulares Informativas___ Correo Electrónico___
Comunicación a través de charlas y reuniones___ Otro___

4. ¿Recibe capacitaciones acerca del manejo y actualizaciones de la plataforma Moodle?

Nunca____ casi nunca_____ a menudo_____ muy a menudo_____

5. ¿Existe un inventario de activos?

SI____ NO_____ NS/NC_____

6. ¿Se ha realizado y documentado una evaluación de riesgo de la información de la plataforma?

SI____ NO_____ NS/NC_____

7. ¿Firmó un acuerdo de confidencialidad o de no divulgación respecto al tratamiento de la información de la plataforma?

SI____ NO_____

8. ¿Existen procedimientos para comunicar anomalías en la plataforma?

SI____ NO_____ NS/NC_____

9. ¿Conoce algún Plan de Emergencia que organice y defina las actuaciones, (quien debe actuar, con qué medios, que se debe hacer, qué no se debe hacer, como se debe hacer), frente a una catástrofe natural que pueda presentarse en la dependencia?

SI___ NO___

10. ¿Cuándo fue la última vez que recibió una capacitación en el uso de equipos contra incendios?

Hace dos años___ Hace un año___ Hace seis meses___ Nunca___ Otro___

11. ¿Existen normas y procedimientos para Control de Acceso a la plataforma?

SI____ NO_____ NS/NC_____

12. ¿Existen normas que determinen el uso de contraseñas seguras?

SI___ NO___

13. ¿Existen procedimientos para la activación y desactivación del derecho de acceso a redes?

SI____ NO_____ NS/NC_____

14. ¿Se controlan los cambios en los sistemas y en los recursos de tratamiento de la información?

SI____ NO_____ NS/NC_____

15. ¿Están definidos los procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento?

SI____ NO_____ NS/NC_____

16. ¿Se tiene implementado controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios?

SI____ NO_____ NS/NC_____

17. ¿Se mantiene un control de versiones para todas las actualizaciones de la plataforma?

SI____ NO_____ NS/NC_____

18 ¿Conoce la existencia de un Plan de Contingencia y su propósito?

SI___ NO___

19. ¿Cuándo fue la última vez que recibió una capacitación en seguridad informática y/o seguridad de la información?

Hace dos años___ Hace un año___ Hace seis meses___ Nunca___ Otro___

20. ¿Usted ha laborado en horarios fuera de su trabajo en el departamento de cómputo?

SI___ NO___ Por qué?_____

21. ¿Ha recibido capacitación en el desempeño de sus funciones, para saber cómo actuar luego de presentarse incidentes o crisis?
SI___ NO___

22. Existen mecanismos para evitar la interrupción de los servicios por fallos de energía?

SI___ NO___ Cuáles_____