PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-FODESEP 2023

PROCESO: **GESTION DE CALIDAD**	**Fecha elaboración:** **16/01/2023**	**Fecha actualización:**	**Versión: 1**	**Página:** 1 de 13
Plan de tratamiento de riesgos de seguridad y privacidad de la información 2023	**Elaborado por:** Carlos Andres Silva Moreno Profesional 3 Tecnología		**Aprobado por:** Comité de gestión y Desempeño	
Responsable: Carlos Andres Silva Moreno Profesional 3 Tecnología	**Revisado por:** Andrea Sanabria Parra , Secretaria General		**Código:** GC-FM-018	

TABLA DE CONTENIDO

Contenido

1. INTRODUCCIÓN

El FODESEP realizó una modernización y renovación a la plataforma tecnológica en todos los casos y durante años, buscando una mejora eficaz, eficiente y efectiva para los procesos de la Entidad y como estrategia de apoyo al desarrollo e implementación de su sistema Informático y de información buscando cumplir con su misión y visión.

Dado lo anterior, se debe disminuir los riesgos y siniestros informáticos que se presenten en la entidad, como también reducir la posibilidad de ocurrencia.

En el último año FODESEP registro un incidente informático, debido a que un disco duro de un servidor completo su máximo de almacenamiento y en el momento en el que se quiso ampliar la capacidad de los discos, el servidor por su configuración de RAID presento un error y se desconfiguró la solución raid. Dado lo anterior, no se pudo realizar la instalación del disco duro nuevo y se revirtió todo lo que se había realizado, para que el servidor quedara en su estado anterior.

Teniendo en cuenta que el FODESEP es una entidad vinculada al Ministerio de Educación, donde se adoptara el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno Digital, haciendo necesario poner en marcha un Plan de Seguridad de la Información donde se deben “identificar” aquellos riesgos, que colocan inestable los Servicios Tecnológicos institucionales y la continuidad de estos, se debe orientar los pasos a seguir en caso de presentarse un incidente de estos, que permitirá recuperar la funcionalidad de la plataforma tecnológica, garantizando la continuidad de las operaciones de la Entidad en el cumplimiento misional..

2. OBJETIVOS

2.1 Objetivo General

- Asociar la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información gestionando los riesgos de Seguridad de la información teniendo en cuenta los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad)

2.2 Objetivos Específicos

- Identificar las actividades que actualmente mitigan la presencia de los riesgos estimados.
- Establecer la continuidad o nuevas acciones para retomar el curso normal de operación en caso de presentarse los riesgos valorados.

- Brindar respuesta rápida y oportuna para dar continuidad a las operaciones que componen la infraestructura tecnológica.
- Procurar que la restauración de los servicios de informática y tecnología sean con un impacto mínimo de costo / pérdida para la entidad.

3. ALCANCE

En virtud de lo planteado en la guía, la identificación del riesgo se hace con base en causas identificadas para los procesos, dichas causas pueden ser internas o externas, según lo que haya identificado la Entidad a través del Contexto estratégico.

En esta parte es importante la participación del personal elegido para la implementación del MSPI, en la mesa interdisciplinaria en la cual se revisan los procesos, haciendo parte de la identificación de los riesgos de seguridad, para los procesos identificados como críticos dentro del planteamiento del MSPI.
Inicia con la definición de algunos términos que son necesarios dentro del empleo de esta metodología, son los relacionados a continuación:

- Proceso.
- Objetivo del Proceso.
- Identificación de Activos.
- Riesgo.
- Causas (Amenazas y Vulnerabilidades).
- Descripción del Riesgo.
- Efectos de la materialización del Riesgo.

Luego se debe realizar la clasificación de los riesgos, para el caso del FODESEP se hará la identificación de "**Riesgos de Tecnología**", teniendo en cuenta los pilares de la seguridad de la información:

- Disponibilidad
- Confidencialidad
- Integridad

4. RESPONSABLE

- Profesional 3 de Tecnología

5. REVISIÓN Y ACTUALIZACIÓN

El plan de Mantenimiento se medirá por la identificación de riesgos y aseguramiento del os mismos en la matriz de riesgo operativo.

6. METODOLOGÍA PARA LA FORMULACIÓN DEL PLAN

Para el plan de tratamiento de riesgos de seguridad y privacidad de la información-fodesep 2023, se tuvo en cuenta.

- Análisis de riesgos
- Identificación de Riesgos
- Identificación de Amenazas
- Identificación de controles

7. MEDICIÓN E INDICADORES

A continuación, se muestran una sucesión de etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas la norma ISO 27005.

IDENTIFICACIÓN DEL RIESGO

La intención de la identificación del riesgo es establecer que podría pasar en caso de que suceda una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida. Las siguientes etapas deberían recolectar datos de entrada para esta actividad.

IDENTIFICACIÓN DE LOS ACTIVOS

Conforme a la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se deberá llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. Para realizar esta identificación es necesario revisar la guía de gestión de activos adjunta al MSPI.

IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daño a activos como: La información, procesos y sistemas por lo tanto las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas, por ellos es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo.

Las amenazas pueden afectar a varios de un activo y en algunos casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

A continuación, se describen una serie de amenazas comunes.
D= Deliberadas, A= Accidentales, E= Ambientales

Para los riesgos tecnológicos que se identificaran, se tendrá en cuenta las probables amenazas comunes y las amenazas humanas que apliquen al FODESEP.

- **Fuentes de amenazas comunes**

TIPO	**AMENAZA**	**ORIGEN**
PERDIDA DE LOS SERVICIOS ESENCIALES	Fallas en el sistema de suministro de aire acondicionado	D A
	Perdida de suministro de energía	A
	Falla en la capacidad de almacenamiento	D A
	Falla en equipo de telecomunicaciones	D A
Compromiso de la información	Hurto de equipo	A
	Manipulación con hardware	A
	Manipulación con software	A

TIPO	AMENAZA	ORIGEN
Fallas técnicas	Fallas del equipo	A E
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	D A
Acciones no autorizadas	Uso no autorizado del equipo	D A
	Uso de software falso o copiado	D A
	Corrupción de los datos	D A
	Procesamiento ilegal de datos	D A
	Copia fraudulenta del software	D A

- **Fuentes de amenazas humanas**

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
	Dinero	
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación	• Penetración en el sistema • Manipulación en el sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

IDENTIFICACIÓN DE CONTROLES EXISTENTES

Algunos controles que se van a tener, para evitar riesgos o amenazas a la plataforma tecnológica son:

- Borrador POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
- Realizar una vez al año como mínimo auditorías internas, para control de licenciamiento institucional, uso de Internet, y demás, en cumplimiento de la Política de seguridad y privacidad de la información.
- control de DERECHOS DE AUTOR de licenciamiento institucional.
- Bloqueo de permisos en el directorio activo en la red interna del FODESEP.

IDENTIFICACIÓN DE LAS VULNERABILIDADES

Lo que nos aplica y se identificaran vulnerabilidades en el área “Hardware, software y equipos de comunicaciones”.

Vulnerabilidades identificadas en el proceso de Tecnología y métodos para la valoración de la misma.

TIPO DE ACTIVO	***VULNERABILIDADES***	***AMENAZAS***
SERVIDOR	ACCESO A INTERNET	HACKING
SOFTWARE CYGNUS	VERSIONAMIENTO 2008	DAÑO EN BDE INFORMACION
INFORMACION EQUIPOS	PERDIDA DE INFORMACION	BORRADO ACCIDENTAL DE INFORMACION
DAÑO EQUIPOS	DAÑO POR GOLPES	MOVILIZACION DE PORTATILES

8. ANEXO 1 CRONOGRAMA

9. ANEXO 2 PRESUPUESTO

FONDO DE DESARROLLO DE LA EDUCACIÓN SUPERIOR -FODESEP-
PLAN DE MANTENIMIENTO DE TECNOLOGÍAS DE LA INFORMACIÓN 2023
CRONOGRAMA DE ACTIVIDADES

MINISTERIO DE EDUCACIÓN NACIONAL

ACTIVIDAD	AÑO 2023											
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Mantener activa y actualiza la solución de antivirus. Firewall actualizado y con políticas restrictivas. Procedimiento Instalación de software y servicios.			x									
Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Solución de Backus automatizada y en la nube. Política de Seguridad aplicada. Exigir estándares de desarrollo y acuerdos de							x					
Política de Seguridad aplicada. Firewall con políticas de seguridad activas. Administración controlada de la red de datos. Procedimiento Instalación de software y servicios. Copia de respaldo (backup) y restauración de la información de los equipos de cómputo. Administración de claves de servidores y								x				
Solucion de backup de la base de datos de Apoteosys					x							

FONDO DE DESARROLLO DE LA EDUCACIÓN SUPERIOR -FODESEP-
CRONOGRAMA DE ACTIVIDADES
PLAN DE MANTENIMIENTO DE TECNOLOGÍAS DE LA INFORMACIÓN 2023

MINISTERIO DE EDUCACIÓN NACIONAL

AÑO 2023

ACTIVIDAD	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	
PRESUPUESTO DE ACTIVIDADES													**Total**
Mantener activa y actualiza la solución de antivirus. Firewall actualizado y con políticas restrictivas. Procedimiento Instalación de software y servicios.				$ 4.500.000,00									$ 4.500.000,00
Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Solución de Backus automatizada y en la nube. Politica de Seguridad aplicada. Exigir estándares de desarrollo y acuerdos de confidencialidad. Procedimiento Instalación de software y servicios. Copia de respaldo (backup) y restauración de la información de los equipos de cómputo. Administración de claves de servidores y equipos. Actualizaciones técnicas a los servidores.							$ 16.500.000,00						$ 16.500.000,00
Politica de Seguridad aplicada. Firewall con políticas de seguridad activas. Administración controlada de la red de datos. Procedimiento Instalación de software y servicios. Copia de respaldo (backup) y restauración de la información de los equipos de cómputo. Administración de claves de servidores y equipos.													$ -
Solucion de backup de la base de datos de Apoteosys					$ 7.500.000,00								$ 7.500.000,00
													$ -
													$ -
													$ -
													$ -
Total	$ -	$ -	$ -	$ 4.500.000,00	$ 7.500.000,00	$ -	$ 16.500.000,00	$ -	$ -	$ -	$ -	$ -	$ 28.500.000,00