PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Vigencia 2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de seguridad y privacidad de la información. del FODESEP, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planeen acciones que reduzcan la afectación a la entidad en caso de materialización, adicionalmente busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC del FODESEP

2. OBJETIVO

2.1 Objetivo General

Definir la ruta de trabajo para la gestión de riesgos de seguridad de la información/digital que, permita mantener la integridad, confidencialidad y disponibilidad de la información mediante la gestión de riesgos asociados a los activos de información del FODESEP.

2.2 Objetivos Específicos

- Asociar la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información
- Gestionar los riesgos de Seguridad de la información teniendo en cuenta los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad)
- Reconocer las situaciones de riesgo que pueden afectar la infraestructura informática, las actividades que minimizan la materialización de dichos imprevistos y poder actuar en fin de la continuidad de la operación de la plataforma tecnológica Institucional.
- 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.
  Velar que la restauración de los servicios de informática y tecnología sean con un impacto mínimo de costo / pérdida para la entidad

3. ALCANCE

La gestión de riesgos de seguridad de la información, incluido su tratamiento será aplicado sobre todos los activos de información del FODESEP; con base en las normas vigentes, la metodología definida por el FODESEP para la gestión del riesgo definida, las pautas y recomendaciones

previstas en la ISO 27001 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

4. RESPONSABLE

El responsable del cumplimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información de la información es el Líder Gestor TI e Infraestructura.

5. REVISIÓN Y ACTUALIZACIÓN

El encargado de realizar el monitoreo, seguimiento y control del plan de acuerdo con la competencia y la normatividad vigente es el Líder Gestor TI e Infraestructura en caso de tener actualizaciones del plan el comité institucional de gestión y desempeño aprobara los respetivos cambios.

6. MARCO NORMATIVO

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1078 del 26 de mayo del 2015 “Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones”
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Resolución 500 del 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013
- Norma Técnica Colombiana NTC-ISO 31000:2011
- CONPES 3854 de 2016. Política Nacional de Seguridad digital

7. METODOLOGÍA PARA LA FORMULACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Identificación de Riesgos

En virtud de lo planteado en la guía de gestión de riesgos de la identificación del riesgo de MINTIC, 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 de los empleados para la implementación del Marco de Seguridad del Modelo de Seguridad y Privacidad de la información 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

Posterior 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

ANÁLISIS DE RIESGOS

A continuación, se describen 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
Fallas técnicas	Fallas del equipo	A
	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 Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema

	Alteración no autorizada de los datos	
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

Controles existentes, para evitar riesgos o amenazas a la plataforma tecnológica son:

- Política de seguridad y privacidad de la información.

- Realización de auditorías internas, para control de licenciamiento institucional, uso de Internet, y demás, en cumplimiento de la Política de seguridad y privacidad de la información.
- Bloqueo de permisos en el directorio activo en la red interna del FODESEP

IDENTIFICACIÓN DE LAS VULNERABILIDADES

Se identificarán vulnerabilidades en el área Hardware y software

TIPO DE ACTIVO	VULNERABILIDADES	AMENAZAS
Servidor	Acceso a internet	Hacking
Software Apoteosys	Versión antigua	Daño en BD información
Información equipos	Perdida de información	Borrado accidental de información
Daño equipos	Daño por golpes	Movilización de portátiles

Análisis del Riesgo

TIPO ACTIVO	PROBABILIDAD / VULNERABILIDAD	IMPACTO / AMENAZA	ACCIONES PREVENTIVAS/CORRECTIVAS	EJECUCIÓN
SERVICIO DE INTERNET, SERVIDORES, SWITCH, ROUTER, REDES LAN, Wfi: Ataques a la plataforma informática	Ataques pueden ser internos o externos por: Deficiencia o falta de una Política de Seguridad Informática institucional definida. Correctamente para el uso los Sistemas Informáticos del FODESEP. Herramientas de Seguridad Perimetral poco eficaces en hardware y software en la construcción e implantación de	Accesos no autorizados por parte de “delincuentes informáticos” u otros con pretensiones de causar daños potenciales a la Red informática del FODESEP y datos contenidos en estos, mediante ataques a los sistemas que componen la	Mantener activa y actualiza la solución de antivirus. Firewall actualizado y con políticas restrictivas.	Octubre 2024

	Políticas eficaces en el FODESEP.	Plataforma Informática.		
SERVIDORES INSTITUCIONALES: Pérdida de información en los Servidores	Falta de mantenimiento preventivo y correctivo a los Sistemas de: equipos Servidores. Sistema eléctrico regulado UPS´s y a la red LAN. Servidores que componen la Planta Informática. Desconocimiento de los Ingenieros Por desconfiguración en equipos. Ausencia de un sistema de Backup´s Falta tercerizar los servicios en la NUBE Soportes poco idóneos. Ausencia de Políticas de Seguridad Informática para los Servidores. Desarrollos inadecuados de aplicativos o implementaciones mal realizadas. Obsolescencia.	Daños físicos o lógicos en los servidores institucionales. Caída de la red LAN Fallo en el Fluido eléctrico regulado por UPS Propagación de virus o programas basura como SPAM Daños en aplicativos y/o Base de datos. Daños físicos en discos duros. Alteración de los desarrollos de los aplicativos. Caídas del servicio de Internet	Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Solución de Backus automatizada y en la nube. 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,	Agosto y Septiembre 2024

EQUIPOS DE COMPUTO: Falla de equipos electrónicos y hardware.	Ausencia de Políticas claras y definidas en el uso correcto de equipos electrónicos y de Hardware. Planes de Mantenimiento preventivo y correctivo anuales a la Planta Informática del FODESEP. Adecuación completa de una red eléctrica regulada en el 100% del FODESEP que cumpla con normas vigentes para la protección entre otros de equipos electrónicos.	Estas se pueden dar por: Cumplimiento de vida útil de un equipo de cómputo. Uso continuo de equipo electrónico. Falta de Mantenimientos Preventivos y Correctivos No se cuenta con una red eléctrica regulada o completa. Ineficiente cantidad de UPS Mal uso por parte de los responsables de los equipos	Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Política de Seguridad aplicada. Copia de respaldo (backup) y restauración de la información de los equipos de cómputo.	Agosto y Septiembre 2024
UPS Y RED REGULADA: Fallas en el suministro de Energía Eléctrica Regulada o UPS (Sistemas de Poder Ininterrumpido) y Red Alambrada	Por falta de mantenimiento preventivo y correctivo a la Planta de UPS actuales y el sistema de tomas eléctricas de los puestos de trabajo. Políticas no existentes o poco claras en su uso. Inestabilidad de la UPS por sobrecarga. Deficientes conexiones en tomas eléctricas reguladas.	Se puede dar por: Deficiencia de UPS para mantener los servicios por un tiempo razonable en los equipos. Sistema de UPS poco confiables Conexiones inadecuadas en tomas eléctricas de puestos de trabajo Malas conexiones de las UPS Niveles de carga eléctrica mayores a los	Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Adquisición de planta eléctrica.	Agosto y Septiembre 2024

		soportados por la Red Eléctrica o las UPS Ausencia de Línea a Tierra (GND) Calidad del cableado eléctrico ineficiente o poco confiable.		
TELEFONÍA IP: Caídas del servicio telefónico IP	Por falta de: Mantenimiento a los equipos del servicio. Soporte al aplicativo telefonía IP y sus funcionalidades. Obsolescencia.	Se puede dar por: Caída del Servidor. Fallo en la Fibra Óptica del proveedor o en los equipos Router del operador. Desconexiones de Red en los teléfonos IP. Fallos en Red LAN. No renovación de contrato de proveedor de servicio del canal dedicado de internet.	Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica. Actualización de software telefonía IP. Tener un servicio de internet contingente con otro operador.	Agosto y Septiembre 2024

RED DE DATOS: Fallos de la Red de Datos por una mala instalación o cortos presentados en esta.	Por falta de: Ausencia de una política de Red de Datos. Certificación de la Red institucional. Maquillaje o identificación de puntos de red. Organización correcta de puntos de datos en el Centro de Datos. Mantenimiento a los dispositivos de redes como Switch. Reorganización del cableado de datos Certificación de la red de datos Redistribución de puntos	Se puede dar por: Corto en Puntos de Datos. Congelamiento de la red por daños. Dispositivos Switch en mal estado. Cables en mal estado. Deficiente distribución por pisos. Pachtcord o Crossover hechos manualmente. Manipulación inadecuada de los cables.	Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica.	Agosto y Septiembre 2024
PÁGINA WEB INSTITUCIONAL: Manipulación indebida de los archivos fuentes y bases de datos de la página WEB	Pérdida de Control en el manejo de la página WEB. Accesos no autorizados Manipulación de los datos	No habría control total de los archivos fuentes y las bases de datos	Acuerdos de confidencialidad. Solución de Backup´s (diarios, semanales).	Febrero 2024
INFORMACIÓN INSTITUCIONAL: Sustracción no autorizada de Datos e información institucional	Puede ocurrir por: Falta de lineamientos en cuanto a responsabilidades del manejo de la información. Controles poco eficientes en accesos no autorizados - Exceso de confianza en el manejo de las responsabilidades	Se puede dar por: Personal no autorizado tiene acceso no autorizado a los sistemas informáticos, equipos de cómputo, servidores, archivos importantes, lo que convierte la Plataforma Tecnológica en algo muy sensible a pérdidas,	Firewall con políticas de seguridad activas. Administración controlada de la red de datos.	Febrero 2024

		alteración, daño o robos de información.		
HARDWARE Y SOFTWARE: Daños en equipos y/o el software por el ataque de virus informáticos	Puede ocurrir por: Falta de políticas en el uso de Software Ausencia de un programa antivirus en los equipos Deficiente administración del Antivirus Actualizaciones no realizadas Desactivación del antivirus	Propagación de programas o rutinas dañinas que afecten los sistemas informáticos.	Solución de antivirus actualizada. Firewall actualizado y con políticas.	Marzo 2024
INFRAESTRUCTURA INFORMÁTICA: Sabotaje / vandalismo	Deficiencias en el control de ingreso no autorizados a los Centros de Datos o equipos de red ubicados en diferentes sitios a este y que carecen de seguridad, lo que pueden ser manipulables por cualquiera.	El Centro de Datos se encuentra dispuesto en dos espacios físicos diferentes en la entidad, en razón a esto, se dificulta controlar el acceso de personas que puedan alterar el normal funcionamiento de los sistemas informáticos.	Se tiene un control de acceso al centro de datos, se debe tener mínimo configurada el uso de dos tarjetas inteligentes, asignadas a 2 funcionarios para el acceso diferentes claves de servidores y equipos. Respaldo del centro de datos externo de la sede principal del FODESEP, donde está actualmente el centro de datos principal.	Febrero 2024

INFRAESTRUCTURA INFORMÁTICA: Desastres naturales / Conflagraciones, inundaciones, movimientos telúricos que afecten la infraestructura informática.	El FODESEP, no está exento de que se pueden presentar cortos en las tomas eléctricas, por ende, recalentamiento en equipos, o hechos más graves como conflagraciones que afecten los equipos y redes informáticos. Los equipos de cómputo, la red eléctrica regulada, la red LAN (canaletas) puede sufrir daños, causados por inundaciones al presentarse rupturas en la tubería del agua. La presencia de los movimientos telúricos es alta e impredecible, lo que provocaría que en el FODESEP se presente catástrofe en la infraestructura física, de acuerdo a estudio realizado por la Universidad Nacional donde la edificación principal no cumple con normas de sismo resistencia, afectando por ende la infraestructura informática	Incendios, inundaciones, movimientos telúricos que afecten la infraestructura informática provocando daños en la misma (perdida de información, daños en equipos que generen parálisis en la gestión institucional)	Plan de contingencia con solución de Backups en la nube. Copia de respaldo (backup) y restauración de la información de los servidores.	Octubre 2024

Matriz de análisis de riesgo cualitativo

Probabilidad	Impacto				
	Insignificante 1	Menores 2	Moderados 3	Mayores 4	Catastróficas 5

A (casi certeza)	A	A	E	E	E
B (probable)	M	A	A	E	E
C (moderado)	B	M	A	E	E
D (improbable)	B	B	M	A	E
E (raro)	B	B	M	A	A

Aplicación Matriz y calificación de los riesgos

Riesgo	Probabilidad	Impacto	Calificación
Servicio de Internet, Servidores, Switch, Router, redes LAN, Wifi. **Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia BAJA**	D	2	**B**
Pérdida de información en los Servidores **Evaluado el riesgo y lo que actualmente ha hecho se ha hecho para reducir este, es de ocurrencia ALTA**	B	2	**A**
Falla de equipos electrónicos y Hardware **Evaluado el riesgo y lo que actualmente ha hecho se ha hecho para reducir este, es de ocurrencia MODERADO**	C	2	**M**
Fallas en el suministro de Energía Eléctrica Regulada	B	3	**A**

o UPS (Sistemas de Poder Ininterrumpido) **Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia ALTA**			
Caídas del Servicio Telefónico IP **Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia MODERADO**	C	2	**M**
Fallos de la Red de Datos **Evaluado el riesgo y lo que se ha hecho para reducir este, es de ocurrencia ALTA**	C	3	**A**
Página WEB institucional **Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia ALTA**	C	3	**A**
Robo común de Datos e información institucional **Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia MODERADO**	B	2	**M**
Equipos de virus informáticos **Evaluado el riesgo y lo que se ha hecho para reducir este, es de ocurrencia MODERADO**	C	2	**M**
Fallas de personal "clave" de Informática	B	3	**A**

Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia ALTO			
Sabotaje / vandalismo Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia ALTO	B	2	**A**
Conflagraciones, inundaciones, movimientos telúricos que afecten la infraestructura informática. Evaluado el riesgo y lo que actualmente se ha hecho para reducir este, es de ocurrencia ALTO	B	3	**A**

8. MEDICIÓN E INDICADORES

Actividades programadas, sobre actividades realizadas

9. REFERENCIA BIBLIOGRÁFICA

- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Departamento Administrativo de la Función Pública 2020.
- Guía de gestión del riesgo, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Guía de orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, territoriales y sector público, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

10. ANEXO 1 CRONOGRAMA

Anexo

11. ANEXO 2 PRESUPUESTO

Anexo

FONDO DE DESARROLLO DE LA EDUCACIÓN SUPERIOR	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código	GCA-FO-14
		Versión	1
		Fecha	23/11/2023

FONDO DE DESARROLLO DE LA EDUCACIÓN SUPERIOR	FORMATO CRONOGRAMA DE ACTIVIDADES PLAN INSTITUCIONAL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código	GCA-FO-02
		Versión	1
		Fecha	11/22/2023

ACTIVIDAD	AÑO 2023											
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológicaa los servidores												
Analisis de riesgo TI contratación Ethical Hacking												
Solución de Backup automatizada y en la nube.												
Política de Seguridad aplicada.												
Actualizaciones técnicas a los servidores.												
Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica Equipos de computo												
restauración de la información de los equipos de cómputo.												
Contratar mantenimientos preventivos y correctivos de toda la UPS												
Contratar mantenimientos preventivos y correctivos de toda la plataforma de la red regulada												
Adquisición de planta eléctrica.												
Contratar mantenimientos preventivos y correctivos de toda la plataforma de telefonia IP.												
Actualización de software telefonía IP.												
Contratar servicio de internet contingente												
Contratar mantenimientos preventivos y correctivos de toda la plataforma de la red de datos												
Contratar mantenimientos preventivos y correctivos del aire acondionado centro de datos												
Acuerdos de confidencialidad Pagina WEB institucional												
Solución de Backup´s Pagina WEB institucional												
Firewall con políticas de seguridad activas												
Administración controlada de la red de datos												
Solución de antivirus Sophos actualizada.												
Firewall actualizado												
Configuracion segunda tarjeta de acceso a centro de datos												
Plan de contingencia con solución de Backups en la nube.												
Copia de respaldo (backup) y restauración de la información de los servidores.												

NOTA: De realizar su plan por proyectos por favor colocar tÍtulo así:

FONDO DE DESARROLLO DE LA EDUCACIÓN SUPERIOR	FORMATO PRESUPUESTO DE ACTIVIDADES PLAN INSTITUCIONAL PLAN INSTITUCIONAL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código	GCA-FO-03
		Versión	1
		Fecha	11/22/2023

AÑO 2023

ACTIVIDAD	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	
	PRESUPUESTO DE ACTIVIDADES												**Total**
Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológicaa los servidores								$ 12,000,000.00					$ 12,000,000.00
Analisis de riesgo TI contratación Ethical Hacking		$ 6,000,000.00											$ 6,000,000.00
Solución de Backup automatizada y en la nube.		$ 15,000,000.00											$ 15,000,000.00
Política de Seguridad aplicada.			$ -										$ -
Actualizaciones técnicas a los servidores.								$ 10,000,000.00					$ 10,000,000.00
Contratar mantenimientos preventivos y correctivos de toda la plataforma tecnológica Equipos de computo								$ 11,000,000.00					$ 11,000,000.00
Copia de respaldo (backup) y restauración de la información de los equipos de cómputo.								$ 2,500,000.00					$ 2,500,000.00
Contratar mantenimientos preventivos y correctivos de toda la UPS								$ 1,500,000.00					$ 1,500,000.00
Contratar mantenimientos preventivos y correctivos de toda la plataforma de la red regulada		$ 3,000,000.00											$ 3,000,000.00
Adquisición de planta eléctrica.							$ 8,000,000.00						$ 8,000,000.00
Contratar mantenimientos preventivos y correctivos de toda la plataforma de telefonia IP.		$ 4,000,000.00											$ 4,000,000.00
Actualización de software telefonía IP.		$ 15,000,000.00											$ 15,000,000.00
Contratar servicio de internet contingente			$ 2,400,000.00										$ 2,400,000.00
Contratar mantenimientos preventivos y correctivos de toda la plataforma de la red de datos		$ 3,000,000.00											$ 3,000,000.00
Contratar mantenimientos preventivos y correctivos del aire acondionado centro de datos								$ 2,000,000.00					$ 2,000,000.00
Acuerdos de confidencialidad Pagina WEB institucional			$ -										$ -
Solución de Backup´s Pagina WEB institucional		$ 1,500,000.00											$ 1,500,000.00
Firewall con políticas de seguridad activas													$ -
Administración controlada de la red de datos						$ -							$ -
Solución de antivirus Sophos actualizada.			$ 6,000,000.00										$ 6,000,000.00
Firewall actualizado											$ 6,000,000.00		$ 6,000,000.00
Configuracion segunda tarjeta de acceso a centro de datos													$ -
Plan de contingencia con solución de Backups en la nube.		$ 16,000,000.00											$ 16,000,000.00
Copia de respaldo (backup) y restauración de la información de los servidores.		$ -											$ -
Total	$ -	$ 63,500,000.00	$ 8,400,000.00	$ -	$ -	$ -	$ 8,000,000.00	$ 39,000,000.00	$ -	$ -	$ 6,000,000.00	$ -	$ 124,900,000.00