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

1. OBJETIVO

El Instituto Tecnológico del Putumayo, en contexto con las políticas nacionales del Ministerio de Tecnologías de la Información y Comunicaciones; pone a disposición el siguiente procedimiento para el tratamiento de riesgos de seguridad y privacidad de la información.

Este documento tiene como objetivo establecer los procesos mínimos a seguir para un óptimo tratamiento de los riesgos de la seguridad y privacidad de la información, se basa en las actividades realizadas por la institución en materia de monitoreo de la estrategia de Gobierno en línea, el cual busca almacenar los datos de los ciudadanos garantizando la privacidad y seguridad de la información.

2. ALCANCE

El programa de tratamiento de la seguridad y privacidad de la información, aplica para todas las dependencias del Instituto Tecnológico del Putumayo.

3. JUSTIFICACIÓN

Todos los servidores públicos y contratistas del estado, en cumplimiento de sus funciones, están sometidos a riesgos que pueden ocasionar la perdida de información y con ello, generar retrasos e inconvenientes en el desempeño de las tareas asociadas a sus obligaciones; por lo tanto, es trascendental tomar las medidas necesarias para identificar las causas y prevenir las consecuencias de la materialización de dichos riesgos.

4. DEFINICIONES Y SIGLAS

4.1 DEFINICIONES

- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de información**: Son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.
- **Alta dirección**: Es como se les denomina a los directivos con más alto cargo en una organización de la empresa y está conformado en el siguiente orden jerárquico que es: el Presidente, el Rector, el Gerente General y los Directores de las distintas áreas o dependencias.
- **Administración de riesgos**: Conjunto de etapas secuenciales que se deben desarrollar para un adecuado tratamiento de los riesgos.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis del riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Antivirus**: Es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus.
- **Calificación del riesgo**: Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Causa**: Medios, circunstancias y/o agentes que generan riesgos.
- **Circuito eléctrico**: Es el recorrido establecido de antemano que una corriente eléctrica tendrá. Se compone de distintos elementos que garantizan el flujo y control de los electrones que conforman la electricidad. Los circuitos eléctricos están presentes en toda instalación que haga uso de energía eléctrica.

- **Ciberdelincuencia**: Se define como cualquier tipo de actividad en la que se utilice Internet, una red privada o pública o un sistema informático domestico con objetivos como destruir o dañar ordenadores, medios electrónicos y redes de Internet.
- **Configuración**: Es un conjunto de datos que determina el valor de algunas variables de un programa o un sistema operativo.
- **Consecuencia**: Se refiere a los efectos producidos gracias a la materialización de un riesgo.
- **Consola KVM**: Es un dispositivo hardware que permite al usuario controlar múltiples servidores de datos desde uno o más conjuntos de teclados, monitores de vídeo, y ratones.
- **Contexto estratégico**: Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Contraseña**: Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.
- **Control**: acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Copia de seguridad**: También conocida como respaldo, copy backup, copia de respaldo, copia de reserva en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales; etc.
- **Copia espejo**: Se conoce como copia espejo (en inglés data mirroring) al procedimiento de protección de datos y de acceso a los mismos en los equipos informáticos implementado en

la tecnología de RAID1. Consiste en la idea básica de tener dos discos duros conectados. Uno es el principal y en el segundo se guarda la copia exacta del principal, almacenando cualquier cambio que se haga en tiempo real en las particiones, directorios, etc., creando imágenes exactas.

- **Credenciales de acceso**: Se refiere a un usuario y contraseña válidos para el acceso a un sistema.
- **Disco duro externo**: Es un dispositivo de almacenamiento de fácil intercambio entre computadores. Suele tener una conexión USB y tiene como finalidad servir de respaldo de datos.
- **Ejecución presupuestal**: Es la etapa del proceso presupuestario en la que se perciben los ingresos y se atienden las obligaciones de gasto de conformidad con los créditos presupuestarios autorizados en los presupuestos.
- **Estados financieros**: También denominados estados contables, informes financieros o cuentas anuales, son informes que utilizan las instituciones para dar a conocer la situación económica y financiera y los cambios que experimenta la misma a una fecha o periodo determinado. Esta información resulta útil para la Administración, gestores, reguladores y otros tipos de interesados como los accionistas, acreedores o propietarios.
- **Evaluación del riesgo**: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Fibra óptica**: Filamento de material dieléctrico, como el vidrio o los polímeros acrílicos, capaz de conducir y transmitir impulsos luminosos de uno a otro de sus extremos; permite la transmisión de comunicaciones telefónicas, de televisión, etc., a gran velocidad y distancia, sin necesidad de utilizar señales eléctricas.
- **Firewall**: Es una aplicación o dispositivo de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno.
- **Hardware**: Conjunto de elementos físicos o materiales que constituyen un computador o un sistema informático.

- **Identificación del riesgo**: Etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- **Información**: Se denomina información al conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado.
- **Internet**: Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen, formen una red lógica única de alcance mundial.
- **Intranet**: Red informática interna de una empresa u organismo, basada en los estándares de Internet, en la que las computadoras están conectadas a uno o varios servidores web.
- **Intrusión**: Acción de introducirse de forma indebida o ilegal en una propiedad, lugar, oficio, asunto, sistema, etc.
- **IPv4**: Es la versión 4 del protocolo IP (Internet Protocol). Es el estándar actual de Internet para identificar dispositivos conectados a esta red. Es uno de los protocolos más importantes para el funcionamiento de internet y fue implementado en ARPANET en 1983.
- **IPv6**: Es la versión 6 del Protocolo de Internet (Internet Protocol), es el encargado de dirigir y encaminar los paquetes en la red, fue diseñado en los años 70 con el objetivo de interconectar redes.
- **Malware**: Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas.
- **Materialización del riesgo**: Ocurrencia del riesgo identificado.
- **Mecanismo de propagación**: Es el método que utiliza una amenaza para infectar un sistema.

- **Medio extraíble**: Hace referencia a algunos dispositivos de almacenamiento extraíbles, cuando éstos son usados para transportar o almacenar datos. Por ejemplo: Memorias USB, Discos duros externos, entre otros.
- **Plan de contingencia**: es un conjunto de procedimientos alternativos a la operatividad normal de cada institución. Su finalidad es la de permitir el funcionamiento de esta, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la organización.
- **Riesgo**: Es el efecto de la incertidumbre sobre los objetivos.
- **Servidor de respaldo**: Es un tipo de servidor que tiene un software de respaldo instalado y tiene mucha capacidad de almacenamiento en discos duros (u otros medios) disponibles para ser usados con el propósito de asegurar que no ocurra pérdida de información.
- **Sistema de enfriamiento**: Se encarga de retirar el exceso de calor generado por los equipos de cómputo, para mantenerlos a su temperatura óptima de trabajo.
- **Sistema de información**: Es un conjunto de datos que interactúan entre sí con un fin común. En informática, los sistemas de información ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.
- **Sistema operativo**: Es el software principal o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software.
- **Sitio web**: Es un conjunto de páginas web desarrolladas en código html, relacionadas a un dominio de Internet el cual se puede visualizar en la World Wide Web (www) mediante los navegadores web.
- **Software**: Conjunto de programas y rutinas que permiten a un equipo de cómputo realizar determinadas tareas.
- **Tecnología de la información**: Se refiere al uso de equipos de telecomunicaciones y computadoras para la transmisión, el procesamiento y el almacenamiento de datos. La noción abarca cuestiones propias de la informática, la electrónica y las telecomunicaciones.

- **Telecomunicaciones**: Sistema de comunicación a distancia que se realiza por medios eléctricos o electromagnéticos.
- **Tesorería**: Es el área de una empresa en la cual se organizan y gestionan todas las acciones relacionadas con operaciones de flujo monetario o flujo de caja.
- **UPS**: Sistema de alimentación ininterrumpida, Uninterruptible Power Supply. Es una fuente de suministro eléctrico que posee un banco de baterías con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.
- **Virus**: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.
- **Vulnerabilidad**: Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.

4.2 SIGLAS

- **TIC**: Tecnologías de la Información y las Comunicaciones.

5. DESARROLLO DEL CONTENIDO

ROLES Y RESPONSABILIDADES FRENTE AL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El éxito en el tratamiento de riesgos de seguridad y privacidad de la información depende de la decidida participación de directivos, servidores públicos y contratistas de la institución, entre los actores que intervienen, están:

- **Alta Dirección**: Aprueban las directrices para el tratamiento de riesgos de seguridad y privacidad de la información en la institución y es la responsable del fortalecimiento de las políticas en torno a ello.
- **Gestión de TIC**: Identifican, analizan, evalúan y valoran los riesgos de seguridad y privacidad de la información en la institución.
- **Servidores públicos y contratistas**: Ejecutar los controles y acciones definidas para el tratamiento de riesgos de seguridad y privacidad de la información, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la institución.
- **Control Interno**: Realiza evaluación y seguimiento a la política, los procedimientos y los controles propios del tratamiento de riesgos de seguridad y privacidad de la información.

POLÍTICA PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Tecnológico del Putumayo adelantará las acciones pertinentes para la implementación y mantenimiento del proceso para el tratamiento de riesgos de seguridad y privacidad de la información, y para ello todos los servidores y contratistas de la institución se comprometen a:

1. Conocer y cumplir las normas internas y externas relacionadas con el tratamiento de riesgos de seguridad y privacidad de la información.

2. Fortalecer la cultura de gestión de riesgos de seguridad y privacidad de la información para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
3. Someter los procesos y procedimientos permanentemente al análisis de riesgos de seguridad y privacidad de la información con base en la aplicación de las metodologías adoptadas para tal efecto.
4. Mantener un control permanente sobre los cambios en la calificación de los riesgos de seguridad y privacidad de la información para realizar oportunamente los ajustes pertinentes.
5. Reportar los eventos de riesgo de seguridad y privacidad de la información que se materialicen, utilizando los procedimientos e instrumentos establecidos para tal efecto.
6. Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos de seguridad y privacidad de la información que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
7. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la institución para así aumentar nuestra eficacia y efectividad.

Para alcanzar la aplicación de las acciones antes definidas, la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, el presente documento forma parte de la política de tratamiento de riesgos de seguridad y privacidad de la información, por cuanto detalla las directrices que deben tenerse en cuenta y que tienen como propósito evitar la materialización del riesgo en la institución.

TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ANÁLISIS DEL CONTEXTO ESTRATÉGICO

El Instituto Tecnológico del Putumayo es una institución pública que tiene a su cargo, la administración de una gran cantidad de activos de información relacionada con diferentes actores como son: estudiantes, docentes, egresados, administrativos y sector productivo, por ende, es necesario mantener el control frente a la exposición a los riesgos de seguridad y privacidad de la información, además de identificar las situaciones generadoras de riesgos que en un momento dado, impidan que actúe en dirección contraria a sus propósitos institucionales.

FACTORES EXTERNOS (AMENAZAS):

- Cambios socio-económicos importantes,
- Catástrofes humanas o naturales,
- Nuevos estándares en materia de manejo de la información,
- Cambios a las leyes y regulaciones,
- Cambios en las demandas de los clientes de la institución,
- Nuevas tecnologías de la información y las comunicaciones,
- Ciberdelincuencia.

FACTORES INTERNOS (DEBILIDADES):

- Cambios en las responsabilidades de la Administración,
- Consideraciones para la contratación y capacitación de personal,
- Acceso de los empleados a la información de carácter institucional,
- Ausencia de políticas claras para la gestión de la seguridad y privacidad de la información,
- Desconocimiento de las recomendaciones mínimas para el acceso a la información de forma segura,
- Resistencia a los nuevos cambios tecnológicos,
- Cambios internos en las tecnologías de la información.

IDENTIFICACIÓN Y CLASIFICACIÓN DE RIESGOS

RIESGOS ESTRATÉGICOS: Se asocia con la forma en que se administra la institución. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- Perdida de información debido a accesos no autorizados o intrusiones por parte de delincuentes informáticos.
- Perdida de información por manipulación indebida de datos, intencional o no intencional.
- Perdida de información por virus informáticos o por la ejecución de programas no autorizados.
- Perdida de equipos informáticos por hurto o por vandalismo.
- Perdida de información y/o de equipos informáticos por incendio en las instalaciones de la institución por desastre natural o de manera intencional.
- No alineación de las políticas institucionales con las políticas nacionales en materia de tratamiento de datos.
- Alteración de información en el sistema académico y/o administrativo y financiero de la institución por accesos no autorizados.

RIESGOS DE IMAGEN: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

- Caídas frecuentes y/o prolongadas por suspensión, mantenimiento o fallas físicas de los servidores que alojan el sitio web de la institución.
- Alteración indebida de información publicada en la página web por usuarios no autorizados.
- Mal manejo de la información para la rendición de cuentas de la institución.

RIESGOS OPERATIVOS: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

- Perdida de información de correos electrónicos institucionales por acceso de usuarios no autorizados.
- Detrimento físico y/o lógico en los servidores de datos de la institución que alojan los sistemas de información SIGEDIN, Moodle, SYS Apolo, Spark, Orfeo, entre otros.
- Daño permanente en los equipos informáticos de telecomunicaciones de la institución por fallas en el circuito eléctrico.
- Fallas de funcionamiento y/o rendimiento en los equipos de cómputo de la institución por infección de virus informáticos, falta de mantenimiento, entre otras causas.
- Alteración de credenciales de acceso a los sistemas de información de la institución.

RIESGOS FINANCIEROS: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

- Pérdida de información financiera por fallas en los equipos de cómputo, infección de virus informáticos, accesos no autorizados.
- Alteración de credenciales de acceso a las entidades bancarias en donde residen las cuentas de la institución por usuarios no autorizados.
- Pérdida de recursos económicos por movimientos fraudulentos en las cuentas bancarias de la institución.
- Falta de transparencia en la gestión de los activos financieros de la institución.

RIESGOS DE CUMPLIMIENTO: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

- Perdida y/o retrasos en la entrega de información a las entidades de control.
- Alteración de la información contractual de la institución por usuarios no autorizados.
- Sanciones por entidades de control debido a retrasos en la entrega de información.

RIESGOS DE TECNOLOGÍA: Están relacionados con la capacidad tecnológica de la institución para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

- Alteraciones y fallas en el circuito eléctrico de la institución.
- Fallas en las fuentes de alimentación ininterrumpida de energía (UPS) de la institución.
- Mal funcionamiento de los dispositivos de protección para evitar el acceso no autorizado o intrusiones por parte de delincuentes informáticos.
- Fallas en el hardware y/o software en los equipos de telecomunicaciones y de cómputo de la institución.
- Ruptura en las conexiones de fibra óptica de la intranet de la institución.
- Caídas del servicio de Internet o bajo rendimiento del mismo.
- Uso incorrecto o desuso del software para la detección, desinfección y/o eliminación de malware.
- Accesos no autorizados a los equipos de cómputo de la institución.
- Fallas en los sistemas de enfriamiento en los cuartos de comunicaciones.

ANÁLISIS DE VULNERABILIDADES

Aunque la protección de la información se ve amenazada frecuentemente por errores cometidos por los usuarios, el Instituto Tecnológico del Putumayo cuenta con otras amenazas e impactos como los siguientes:

1. Algunos puntos de energía no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina del bloque administrativo y la sala docente.

2. El cuarto de comunicaciones principal de la institución, ubicado en el laboratorio de TIC no cuenta con: sistema de enfriamiento, sistema de alimentación ininterrumpida de energía, sistema contra incendios, control de acceso, sistema de cámara de vigilancia, control de temperatura y humedad, piso falso, entre otros.

3. El Firewall, la consola KVM y dos servidores de respaldo adquiridos por el Instituto Tecnológico del Putumayo, aún no se encuentra en funcionamiento.

4. La institución carece de un sistema de copias espejo de la información que residen en los servidores de datos de la institución, así como tampoco cuenta con un sistema de dominio interno.

5. El Instituto Tecnológico del Putumayo carece de un plan para la transición de direcciones IPv4 a IPv6.

6. No existen cuentas de usuario y claves para el acceso de los recursos informáticos en equipos compartidos, asimismo, no existe un sistema que impida que todos los equipos se puedan ver a través de la red.

7. Las dependencias de Bienestar Universitario, Biblioteca, CIECYT, Vicerrectoría Académica, Bilingüismo, Registro y Control Académico, Recursos Físicos y toda el área del pabellón de Laboratorios no cuenta con un sistema ininterrumpido de energía (UPS) adecuado.

8. No existen procesos de copias de seguridad establecidos. Las copias de seguridad se están realizando en forma manual en un disco duro externo. Ésta solución no es óptima, ya que existe riesgo de pérdida total de información en caso de ocurrir desastres naturales, incendios u otros que afecten las copias de respaldo almacenadas en los equipos de cómputo ubicados dentro de la institución.

9. El Instituto Tecnológico del Putumayo no cuenta con el licenciamiento del paquete ofimático Microsoft Office, así como tampoco cuenta con las licencias de una plataforma para el control de malware, aunque ya hay un proceso de adquisición adelantado.

10. Las tres salas de cómputo del Instituto Tecnológico del Putumayo no cuentan con un sistema de protección de los terminales que permitan congelar una instantánea de la configuración deseada de una estación de trabajo y de los ajustes establecidos por el administrador de TI, aunque ya hay un proceso de adquisición adelantado.

11. El Instituto Tecnológico del Putumayo no existe un área de sistemas definida con profesionales encargados de revisar, documentar, diseñar y controlar los procesos propios de un modelo de seguridad y privacidad de la información.

12. No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la institución.

13. Gran parte de los documentos físicos que se manejan en la institución no se han digitalizado, por lo tanto, están expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.

14. Falta de un programa de capacitaciones en el manejo de equipos tecnológicos y sistemas de información.
15. No hay control para el uso de medios extraíbles en los equipos de la institución, exponiendo a perder la información por malware no detectados o daños irreparables del hardware.

16. Gran parte de la información es almacenada y transportada en memorias, discos duros externos y equipos portátiles personales, por ende, la información sale de la institución.

17. Las políticas y normas de seguridad y privacidad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento a

las reglas básicas del cuidado tanto de los equipos informáticos como de la información, algunas son:

- Configuraciones no autorizadas de los sistemas operativos.
- Equipos de cómputo sin contraseñas de acceso o con contraseñas no seguras.
- Contraseñas de acceso a los equipos de cómputo compartidas con compañeros de trabajo.
- Instalación y uso de programas no autorizados o sin el debido licenciamiento.
- Acceso a páginas web no autorizadas.
- Uso de los equipos de cómputo y demás recursos tecnológicos para uso personal y no institucional.
- Consumo de bebidas y alimentos cerca a los equipos de cómputo.

IES vigilada

MINEDUCACIÓN

MATRIZ DE VULNERABILIDADES Y MITIGACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA DE CUMPLIMIENTO: 2018

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	ANÁLISIS Y VALORACIÓN		MITIGACIÓN DEL RIESGO
					CALIFICACIÓN	EVALUACIÓN	
Problemas eléctricos	Las conexiones del bloque administrativo y de la sala docente no son suficientes para la cantidad de equipos de cómputo y dispositivos eléctricos	Inadecuada conexión de cableado eléctrico	Posible pérdida de información	Riesgo tecnológico, físico, humano	2	Riesgo moderado	Plantear un nuevo diseño de la red eléctrica
Perdida de información y de equipos tecnológicos	Cuarto de comunicaciones principal sin sistemas de enfriamiento, UPS, contra incendios, control de acceso, cámara de vigilancia, entre otros	Cuarto sin conexión tomacorriente a 220v, falta de implementación de sistemas alarma y de vigilancia	Posibles fallas y daños permanentes en el hardware	Riesgo tecnológico, físico, de información	4	Riesgo alto	Instalación de conexión a 220v
	Dependencias sin sistema de alimentación ininterrumpida de energía UPS	UPS insuficientes en los inventarios de la institución	Posibles fallas y daños permanentes en el hardware	Riesgo tecnológico, físico, de información	4	Riesgo alto	Reubicación de dependencias y/o adquisición de UPS

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	ANÁLISIS Y VALORACIÓN		MITIGACIÓN DEL RIESGO
					CALIFICACIÓN	EVALUACIÓN	

• **Afectación de activos de información** • **Ataques informáticos** • **Pérdida de información**	Equipos de protección de datos y servidores que aún no han sido instalados	Inexistencia de un profesional encargado de la administración de redes	Ataques informáticos, alteración de información, infección por virus	Riesgo tecnológico	3	Riesgo mediano	Designación de un profesional para la instalación y configuración de equipos
	Equipos de respaldo sin la debida configuración		Pérdida de información	Riesgo de información	4	Riesgo alto	
Perdida de rendimiento en el acceso a Internet	Inexistencia de un plan para la transición de IPv4 a IPv6	En 2011 se agotaron las direcciones IPV4 en el registro central de IANA (Autoridad de Asignación de Números en Internet)	No existen transición de protocolo de IP	Riesgo tecnológico, humano	2	Riesgo moderado	Diseño de plan para la transición del protocolo IP
Perdida de información de funcionarios y de sistemas de información académico, administrativo y financiero	• No existe un proceso de copias de seguridad para la información generada por los sistemas de información y por los distintos funcionarios y contratistas de la institución. • No Existe un sistema de información para la documentación sensible, como contratos y acuerdos.	No hay procesos de copias de seguridad establecidos	Pedida de información, retrasos en el cumplimiento de obligaciones, sanciones legales, inconvenientes financieros, contractuales, entre otros	Riesgo de información, tecnológico y humano	4	Riesgo alto	Diseño de plan de copias de seguridad y definición de tiempos y responsables

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	ANÁLISIS Y VALORACIÓN		MITIGACIÓN DEL RIESGO
					CALIFICACIÓN	EVALUACIÓN	
Problemas legales por uso de software sin licenciamiento	Adquisición de licencias pendiente para el uso del paquete ofimático, de	Falta de recursos para la adquisición de software	Demandas de tipo legal por derechos de autor	Riesgo de información, legal	4	Riesgo alto	Adquisición de licenciamiento de software

	plataformas de protección y de congelamiento						
Incumplimiento de las actividades de seguridad de la información.	Inexistencia de un área de sistemas definida con un equipo de profesionales idóneos	Personal insuficiente para el aseguramiento de la información	Retraso en tiempos de producción para los funcionarios afines a TIC	Riesgo de información, de servicio, tecnológico	3	Riesgo mediano	Conformación del equipo de Gestión de TIC
Desconocimiento de situaciones de riesgo anteriores	Ausencia de historial de reportes de procesos de asistencias y/o mitigación de riesgos	Inexistencia de formato para reportar asistencias y/o mitigación de riesgos	Imposibilidad para llevar un histórico de asistencias y/o mitigación de riesgos	Riesgo de información	1	Riesgo bajo	Diseño de formato para el reporte de situaciones de riesgo
Perdida de información contenida en documentos físicos	Falta digitalización de gran parte de los documentos físicos de la institución	Cantidad de escáneres insuficientes para dicho propósito	Daño de documentos y deterioro del papel	Riesgo de Información	4	Riesgo alto	Adquisición de escáneres y designación de responsables
Manejo inadecuado de equipos tecnológicos y sistemas de información	Inexistencia de un programa de capacitaciones para el manejo de equipos tecnológicos y sistemas de información	Personal insuficiente para diseñar y aplicar capacitaciones en TIC	Ausencia de transferencia de conocimiento y falta de capacitación	Riesgo de Información, tecnológico, en Servicio	3	Riesgo mediano	Creación del plan de capacitaciones en TIC

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	ANÁLISIS Y VALORACIÓN		MITIGACIÓN DEL RIESGO
					CALIFICACIÓN	EVALUACIÓN	
Perdida de información	Desconocimiento de las políticas y normas de seguridad y privacidad de la información	No hay socialización de estos temas	Acciones no adecuadas en el tratamiento de los activos de información e informáticos	Riesgo Tecnológico, en Servicio, personal	3	Riesgo mediano	Establecimiento de políticas y socialización de las mismas

• **Confidencialidad e Integridad de la información** • **Perdida de información**	Utilización de medios extraíbles por parte de funcionarios y contratistas de la institución	Falta de control en los medios extraíbles utilizados al interior de la institución	Incumplimiento de confidencialidad e integridad de la información	Riesgo de información, tecnológico	2	Riesgo moderado	Diseño de controles para el uso de memorias extraíbles

PROPUESTA DE SEGURIDAD

- Realizar un rediseño de la red interna del bloque administrativo y la sala docentes con el objetivo de cambiar la conexión inalámbrica de algunos equipos por cableado estructurado para evitar caídas de Internet.
- Implementar los sistemas de enfriamiento, UPS, sistema contra incendio, control de acceso, cámara de vigilancia, control de temperatura y humedad, entre otros en el Centro de Datos de la institución.
- Instalar y configurar adecuadamente el Firewall, la consola KVM y los dos servidores de respaldo.
- Configurar los servidores para que realicen de copias espejo de la información que residen en los discos duros principales, adicionalmente, configurar un sistema de dominio en la institución.
- Diseñar el plan para la transición del protocolo de direcciones IPv4 a IPv6.
- Crear usuarios y contraseñas por dependencia y configurar todos los equipos de la red de datos de la institución adecuadamente para el acceso de los recursos informáticos en equipos compartidos, asimismo, configurar redes privadas virtuales independientes por nodo con el fin de reducir el dominio de difusión.
- Rediseñar las redes eléctricas de las dependencias de Bienestar Universitario, Biblioteca, CIECYT, Vicerrectoría Académica, Bilingüismo, Registro y Control Académico, Recursos Físicos y toda el área del pabellón de Laboratorios para la adquisición e implementación del sistema ininterrumpido de energía (UPS).
- Diseñar un apropiado sistema de copias de seguridad, migrando en lo posible, al almacenamiento en la nube.
- Adquirir las licencias necesarias del paquete ofimático Microsoft Office, una plataforma que brinde plena confianza en la integridad de los datos y la información que se almacena en los equipos de cómputo y que también permita el control de malware, un sistema de protección de los terminales para las tres salas de computo que permitan

congelar una instantánea de la configuración deseada de las estaciones de trabajo y de los ajustes establecidos por el administrador de TI.

- Conformar el área de sistemas con profesionales encargados de revisar, documentar, diseñar y controlar los procesos propios de un modelo de seguridad y privacidad de la información.
- Diseñar un formato que permita documentar un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la institución.
- Adquirir escáneres de alta velocidad para la digitalización del 100% de los documentos físicos que se manejan en la institución.
- Construir un programa de capacitaciones en el manejo de equipos tecnológicos y sistemas de información de la institución.
- Elaborar un plan para el control del uso de medios extraíbles en los equipos de la institución.
- Definir hasta donde es posible y conveniente que la información institucional salga de la institución en memorias, discos duros externos y equipos portátiles personales.
- Establecer las políticas y normas de seguridad y privacidad de la información y socializarlas con todo el personal.

6. ANEXOS