

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GSI	
		Fecha de Emisión: (15-07-2021)	
	Fecha de Aprobación: ()		
	GESTIÓN DE SISTEMAS DE INFORMACIÓN	Versión: 01	Página: 1 de 7

1. PROPOSITO :

Garantizar el resguardo en forma segura de toda la información digital que dentro del desarrollo de las funciones se considere documental e importante y crítica, generada en cada una de las dependencias de la ESE OCCIDENTE.

2. RESPONSABLE:

Profesional y Técnicos del Área de Sistema de Información

3. ALCANCE:

Aplica para todos los funcionarios de la ESE OCCIDENTE, que tienen a cargo equipos de cómputo y que manejen información importante y crítica. Comprende desde la clasificación de los archivos en las computadoras por parte de cada uno de los usuarios, hasta el almacenamiento de las copias de seguridad.

4. DEFINICIONES Y TERMINOS:

- **COPIA DE SEGURIDAD- (BACKUP):** Se define como backup o copia de seguridad, la actividad de resguardar de forma segura la información contenida en un medio de almacenamiento de origen (disco duro) a un medio de almacenamiento de destino de diferente tipo (otro disco duro, servidor de backup, memoria USB, CD, DVD, ZIP, etc.).
- **INFORMACIÓN IMPORTANTE Y CRÍTICA:** son todos aquellos archivos digitales académico/administrativos generados por el software aplicativo con que cuenta la ESE OCCIDENTE.
- **INFORMACION DOCUMENTAL:** Son todos aquellos archivos digitales institucionales, creados en las computadoras por cada uno de los funcionarios en sus respectivas dependencias.
- **SERVIDOR DE BACKUPS:** Es un equipo de cómputo que formando parte de una red, provee servicios a otros equipos denominados clientes. En este caso servicio de almacenamiento de archivos.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GSI	
		Fecha de Emisión: (15-07-2021)	
	Fecha de Aprobación: ()		
	GESTIÓN DE SISTEMAS DE INFORMACIÓN	Versión: 01	Página: 2 de 7

- **PARTICIÓN:** En computación, una partición de disco es una división lógica de un medio de almacenamiento

- **SISTEMA OPERATIVO:** Un sistema operativo es un software de sistema, es decir, un conjunto de programas de computadora destinado a permitir una administración eficaz de sus recursos.

- **PUERTO USB:** Un puerto USB es una entrada o acceso para que el usuario pueda compartir información almacenada en diferentes dispositivos como una cámara de fotos, un pendrive, entre otros, con un computador. Las siglas USB quieren decir Bus de Serie Universal en inglés.

- **COMPUTADORA:** Es una máquina electrónica que recibe y procesa datos para convertirlos en información útil. Una computadora es una colección de circuitos integrados y otros componentes relacionados que puede ejecutar con exactitud, rapidez y de acuerdo a lo indicado por un usuario o automáticamente por otro programa, una gran variedad de secuencias o rutinas de instrucciones que son ordenadas, organizadas y sistematizadas.

- **VIRUS INFORMÁTICO:** Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

- **MALWARE:** Es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño.

- **FREEWARE:** Define un tipo de software de computadora que se distribuye sin costo y por tiempo ilimitado, siendo una variante gratuita del shareware, en la que la meta es lograr que un usuario pague, usualmente después de un tiempo de prueba ("trial") limitado y con la finalidad de habilitar toda la funcionalidad. (Normalmente se consiguen en Internet).

- **SHAREWARE:** Se denomina a shareware a una modalidad de distribución de software, tanto juegos como programas utilitarios, en la que el usuario puede evaluar en forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso o con restricciones en las capacidades finales. (normalmente se consiguen en Internet).

- **GUSANO INFORMÁTICO:** Es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GSI	
		Fecha de Emisión: (15-07-2021)	
	Fecha de Aprobación: ()		
	GESTIÓN DE SISTEMAS DE INFORMACIÓN	Versión: 01	Página: 3 de 7

- **PROGRAMA ESPÍA:** Spyware, es malware, que se instala en una computadora para recopilar información sobre las actividades realizadas en ella. La función más común que tiene estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.
- **KEYLOGGER:** Es una herramienta que se encargada de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero y/o enviarlas a través de Internet: Suele usarse como malware, permitiendo que otros usuarios tengan acceso a los números de una tarjeta de crédito o a la contraseña de cuentas on line al infiltrarse en un ordenador.
- **SPAM:** Se llama Spam, correo basura o SMS basura a los mensajes no son licitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor
- **FOCOS DE PROPAGACIÓN:** Los principales focos de propagación de virus son: Internet, correos electrónicos con mensajes adjuntos de cadenas, juegos, videos links a otras páginas, Mensajería instantánea externa, ICQ, Chat externo, redes compartidas Punto a punto (Ares, Kazaa, etc.), Memorias USB infectadas.

5. DESARROLLO / PROCEDIMIENTO :

La información de una empresa se ha considerado como un activo fundamental para la prestación de los servicios y la toma de decisiones eficientes, en virtud de ello se requiere contar con estrategias que permitan el control y administración efectiva de los datos.

Dicha información pueda ser sujeta a pérdida, robo, alteración, sustracción o revelación por parte de propios o extraños de manera imprudencial o intencionada, o bien, a sufrir un uso indebido y con ello acarrear daños a su propietario, pueda ser éste un individuo o una organización.

Para resguardarla es fundamental analizarla, evaluarla y clasificarla con el objetivo de determinar el nivel de seguridad que merece, considerando los riesgos a los cuales pueda estar expuesta. Una vez clasificada es preciso llevar a cabo respaldos o soportes, conocidos como "backups" y resguardarla adecuadamente ya sea en archivos de seguridad físicos, discos duros cuyos accesos se encuentren debidamente restringidos con contraseñas robustas.

Conscientes de las necesidades actuales, se hace necesario por parte de la ESE OCCIDENTE implementar Políticas de Seguridad de La Información donde los usuarios incorporen buenas prácticas para proteger seguridad informática y el entorno de información, para ello se deben las recomendaciones, buenas prácticas y demás

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GSI	
		Fecha de Emisión: (15-07-2021)	
	Fecha de Aprobación: ()		
	GESTIÓN DE SISTEMAS DE INFORMACIÓN	Versión: 01	Página: 4 de 7

peligros latentes a nivel de informática, y cómo detenerlos a través de mecanismos de prevención.

➤ **INFORMACIÓN EN UN SISTEMA OPERATIVO**

La técnica más usada para realizar Backups es copiar simplemente los archivos que queremos guardar a otro dispositivo de almacenamiento ya sea una memoria, CD-ROM, DVD, DISCO EXTERNO, Etc. Cuando uno realiza esta copia, lo importante es que los archivos que vaya a copiar, no se estén usando a fin que no genere errores al realizar la copia. El procedimiento no tiene ninguna dificultad simplemente seleccionamos los archivos que queremos copiar y los pasamos al dispositivo que tengamos; al copiar información a un CD o DVD utilizamos como tal el sistema operativo o también programas que nos ayudan a realizarlo. (Solo en el caso de estar licenciados).

Es muy importante tener en cuenta la periodicidad con que se realiza la copia de seguridad, esto depende mucho del manejo de la información en cada dependencia, ya que hay información que se actualiza o se agrega o elimina, muy seguido o también su actualización se realiza esporádicamente.

La copia debe estar lo más actualizada posible, si por ejemplo la información se actualiza diariamente, es bueno tener el hábito de hacer la copia a diario o dependiendo de la actualización sea semanal, quincenal, mensual, etc.

Clasificar la información, esto se hace para que realizar la copia de seguridad no sea un proceso largo y tedioso por la cantidad de información que se está copiando; es necesario hacer una clasificación de la información en donde por un lado tenemos la información que manejamos seguido, esta información debe ser liviana a fin de poder realizar copia de manera rápida; y por otro lado tenemos la información histórica en donde es mucho más robusta y pesada, pero esta información no se modifica periódicamente sino de manera esporádica; de esta manera podemos hacer un backup diario o semanal de la información liviana o la que trabajamos a diario y podemos estipular de manera semestral o anual un backup de toda la información histórica junto con la actual y así tener un repositorio de información organizado y efectivo.

En la clasificación tener los archivos y documentos que son de la dependencia, y son de importancia para la Dependencia; la información personal como son los archivos personales, música y demás, deben estar aparte y cada persona tiene su responsabilidad por dicha información, pero es bueno tener claro la diferencia entre la información laboral y la información personal, porque al realizar una copia al tener esta información mezclada también ocasiona congestión y demoras si se quiere hacer una copia.

La información de los archivos contenidos en las copias de seguridad debe ser única y exclusivamente de uso institucional y no personal.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GSI	
		Fecha de Emisión: (15-07-2021)	
	Fecha de Aprobación: ()		
	GESTIÓN DE SISTEMAS DE INFORMACIÓN	Versión: 01	Página: 5 de 7

Todos los funcionarios de la ESE OCCIDENTE que tienen a cargo equipos de cómputo, que manejen información importante y crítica, deben guardarla en la partición "D" del disco duro de su computadora.

El área de Sistemas de Información y Estadísticas, no se hace responsable por el daño o la pérdida de la información contenida en las computadoras de los usuarios que no realicen sus copias de seguridad al servidor de backup.

El resguardo y almacenamiento adecuado de las copias de seguridad, El área de Sistemas de Información y Estadísticas.

En caso de que algún funcionario necesite copias de sus archivos almacenados en el servidor de backup o en los medios de almacenamiento DVD´s, esta petición debe ser requerida El área de Sistemas de Información y Estadísticas.

➤ **CONSIDERACIONES AL PLAN DE BACKUP**

Cuando se desarrolla un plan de backup se debe tener en cuenta lo siguiente:

- Determinar el tipo de información a ser resguardada, lo que indica que cada copia debe estar debidamente identificada respecto a la información que debe contener.
- Prever los aspectos relacionados con la fiabilidad de la copia, ya que se debe garantizar la integridad de los archivos a ser copiados y de los soportes a utilizar.
- Incluir una prueba de tensión del hardware de backup (unidades de almacenamiento, unidades ópticas y controles) y del software (programas de backup y unidades de dispositivo).

➤ **BASES DE DATOS SERVIDORES**

La información contenida en los servidores de la ESE OCCIDENTE, es de vital importancia; por ello el área de Sistemas de Información y Estadísticas es la única dependencia Autorizada para realizar dichos Backups. El proceso de copias de seguridad debe iniciar automáticamente en cada uno de los servidores de la Institución, el personal encargado de la administración de los servidores debe realizar la recolección de los archivos export que contienen las bases de datos de cada uno de los servidores y unificar las copias, realizando una copia local en el equipo de monitoreo de servidores y otra en el servidor **NAS** de la ESE OCCIDENTE, dicho procedimiento se debe realizar en horas de la mañana y en horas de la tarde. Al final del día se debe grabar en cinta la última copia existente de las Bases de Datos la cual reposara en el cuarto de servidores.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GSI	
		Fecha de Emisión: (15-07-2021)	
	Fecha de Aprobación: ()		
	GESTIÓN DE SISTEMAS DE INFORMACIÓN	Versión: 01	Página: 6 de 7

➤ **RECOMENDACIÓN SOBRE EL USO DEL SOFTWARE**

El personal del Proceso de Sistemas de Información, puede revisar, re-instalar o desinstalar software. Tiene autorización de eliminar software que no cuente con las licencias debidamente registradas y tiene la prohibición expresa de instalar software que no sea proporcionado por la empresa y que se encuentre debidamente licenciado.

Está prohibido realizar copias en CD o USB de archivos que son propiedad de la empresa, para fines externos, solo el jefe podrá realizar copias con conocimiento del jefe de Sistemas de Información

Está prohibido visitar páginas con contenido obsceno, así como bajar programas de internet que no estén permitidos su instalación por parte del área de informática. Todas las páginas visitadas se van a monitorear desde el servidor web.

➤ **SOBRE LA ORGANIZACIÓN DE LA INFORMACIÓN EN UN SISTEMA OPERATIVO.**

Es aconsejable que en los computadores se puedan crear dos particiones. La primera corresponderá al lugar en el cual se instalará el Sistema Operativo, la segunda corresponderá al lugar en el cual se guardarán los demás datos, aunque esto no garantiza la permanencia de la información ni tampoco sea una regla que se deba tener en los computadores, si se facilitan las cosas a la hora de hacer una restauración del computador por daño en el Sistema Operativo, porque simplemente los datos los estamos guardando en una partición y los archivos de programas y demás en donde se encuentra el Sistema Operativo. Si quieren contar con esto es bueno comunicarse con nosotros en el área de Soporte Técnico para que a la hora de instalar el equipo puedan optar por esta opción.

➤ **SOBRE EL NOMBRE DE LOS ARCHIVOS.**

Es muy recomendable que no se guarden archivos con nombres muy largos. Aunque suena extraño esto es vital a la hora de realizar un Backup pues en ocasiones, los archivos que tienen nombres muy largos ocasionan problemas.

Otro punto vital es nombrar los archivos con nombres que nos permitan reconocer que contenido tiene un archivo dado. Esto se hace para no tener que revisar todos los archivos que tenemos en el computador abriéndolos, sino que simplemente nos podremos limitar a leer el nombre del archivo, y con esto debería ser suficiente para decidir si se guarda o se elimina.

Algunos Sistemas Operativos no permiten ingresar unos caracteres especiales al nombre del archivo, pero no está de más sugerirles que no nombren archivos o carpetas utilizando caracteres especiales como (#\$%&?'i'è).

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GSI	
		Fecha de Emisión: (15-07-2021)	
	Fecha de Aprobación: ()		
	GESTIÓN DE SISTEMAS DE INFORMACIÓN	Versión: 01	Página: 7 de 7

En ocasiones, queremos guardar páginas de Internet, guardándolas en formato html. Por lo general estos archivos html que guardamos de Internet, vienen con nombres extremadamente largos y extraños. Así que si queremos guardar información de una página de Internet recomendamos copiar y pegar la información en algún otro archivo.

6. FORMATOS DE REGISTRO:

- Formato Control de Backup Servidores.

7. CONTROL DE REVISION Y APROBACIÓN:

ELABORÓ	REVISÓ	APROBÓ
Nombre: Edward Leao Obando Bravo	Nombre: Eliana García Amu	Nombre: Carlos Alfredo Valverde Zamora
Cargo: Sistemas de Información	Cargo: Subdirectora Administrativa	Cargo: Gerente
Firma:	Firma:	Firma: