

## PLAN DE COPIAS DE SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO DEL INVISBU

**FECHA (16/03/2023)**

### **OBJETIVO**

Efectuar un backup de todos los archivos de datos o documentos generados por las aplicaciones y de todos los archivos de configuración de cada equipo de cómputo del INVISBU.

### **OBJETIVOS ESPECÍFICOS**

- Elaborar y ejecutar el plan de backups de los equipos de cómputo del INVISBU.
- Proteger toda la información institucional de cada equipo de cómputo que posee el instituto.
- Resguardar la información que posee los equipos de cómputo de instituto en caso de presentar riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio Mantener en óptimas condiciones de operatividad los equipos de cómputo y así mejorar su rendimiento.
- Cumplir las Políticas y Estándares de Seguridad Informática.

### **DESARROLLO**

#### **Consideraciones para realizar un Backup**

Teniendo en cuenta los problemas relacionados con los medios de almacenamiento y las razones para hacer backups que se enumeraron anteriormente, se deben prestar atención a determinadas consideraciones sobre el medio destino, que se listan a continuación:

- Debe ser diferente al medio del cual estamos tomando los datos originales (no sirve de mucho almacenar el backup de un disco rígido en ese mismo disco).
- No debe residir en el mismo lugar físico que el medio origen (menos aún en el mismo equipo), pues si ocurre un siniestro o robo en dicho lugar, el backup no habrá servido de nada. Lo ideal es generar varias copias del medio destino y guardarlo en diferentes ubicaciones físicas dispersas, pero no siempre el tiempo y el presupuesto alcanzan; Debemos tener en cuenta que el medio destino también puede presentar fallas a la hora de restaurar los archivos.
- Debe guardarse en un lugar seguro, seco y fresco, teniendo en cuenta a su vez las condiciones del ambiente que requiere el medio para mantener los datos libres de peligro. No deben exponerse al calor, la humedad ni a campos electromagnéticos ya que se podrían dañar.
- Debe etiquetarse en forma ordenada y clara, en donde se incluya la fecha.
- Debe verificarse que los datos almacenados en el mismo son los correctos y se puede acceder a ellos sin inconvenientes.
- Backup es backup. Cuando se habla de backup no nos referimos a cualquier otro mecanismo de recuperación de datos implementado en el sistema, como ser el espejado de discos, replicación de servidores o diferentes configuraciones RAID, sino a la copia de archivos en medios removibles.

**Backup o copia de seguridad:** Se conoce con este nombre al resultado de efectuar una copia de todos, o algunos archivos, que se encuentran en el medio de almacenamiento de una o varias computadoras en otros medios diferentes a este último, para poder recuperarlos en otro momento si se pierden o se dañan Los archivos originales.

#### **Estrategia de Backups**

En algunos casos, solamente necesitaremos efectuar un backup porque vamos a hacer alguna de las tareas enunciadas anteriormente cuando hablamos de circunstancias especiales para resguardar todo. Si de eso se trata, no hace falta demasiada imaginación para definir una estrategia de backup, que va a consistir en armar una copia de resguardo completa de las unidades involucradas en la operación a efectuar. Esto es muy común cuando estamos realizando reparaciones o actualizaciones a un sistema propio o ajeno.

Sin embargo, cuando diseñamos un plan de backups para nuestro sistema o para otra persona o empresa, debemos tener en cuenta algunas estrategias que nos van a ayudar a que el plan sea más conveniente y

## PLAN DE COPIAS DE SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO DEL INVISBU

lograr el mejor costo/beneficio posible, minimizando los tiempos de respuesta, es decir, el tiempo que tardaríamos en recuperar los datos en caso de cualquier desastre.

Al intentar definir un plan de backups, nos surgen dos dudas esenciales:

- ¿Cada cuánto se debería efectuar un backup de los datos? Frecuencia del backup.
- ¿Qué datos se deberían resguardar en cada backup? Datos a resguardar.

### Backup Completo.

Se crea una copia de resguardo de todas las carpetas y archivos que seleccionemos en la herramienta para hacer el backup. Es ideal para crear la primera copia de todo el contenido de una unidad o bien de sus archivos de datos solamente.

Ventajas:

- Todos los archivos seleccionados pasan a formar parte de este backup.
- Para restaurar uno o más archivos, se los toma directamente de este backup.

### ACTIVIDADES PARA REALIZAR UN BACKUP

Las actividades que se van a desarrollar durante el proceso de una copia de seguridad es:

- Informar a los jefes de área del inicio del proceso de la copia de seguridad y mantenimiento correctivo para contar con la disposición y el tiempo para llevar a cabo este proceso. Se debe notificar mínimo con un día de anterioridad al inicio de la fecha programada para el mantenimiento.
- Verificar que el equipo este registrado en el inventario de equipos de cómputo de la institución, esto con el objetivo de corroborar que es de propiedad del Instituto.
- Verificar el estado actual del equipo, al momento de realizar la copia de seguridad.
- Iniciar el proceso de copia de seguridad verificando con cada usuario o responsable de cada equipo de cómputo los archivos, carpetas o documentos que desea guardar en la copia.
- Después de terminar la copia verificar con el usuario o responsable del equipo de cómputo que todo haya quedado en orden.
- Verificar después de haber hecho la copia no haya quedado con errores en el disco extraíble.
- Verificar en el disco extraíble que la copia de seguridad este guardada dentro de la carpeta con el nombre del usuario(equipo)- responsable , y esta a su vez este guarda por fechas de copia.
- Realizar la copia de seguridad de la carpeta en el disco externo asignado este proceso.

### COPIAS DE SEGURIDAD SEMANAL

Se harán copias selectivas en el servidor, disco externo y espacio del hosting de los siguientes archivos:

- Base de Datos "PQRS" del aplicativo de correspondencia ubicado en el SERVER2; el cual se genera desde el Microsoft SQL Server Management Studio Databases\PQRD\Tacks\Backup\ posteriormente se le da OK al procedimiento, el cual deja la copia en: C:\Program Files\ Microsoft SQL Server\MSSQL 14. VENTANILLA\MSSQL\Backup\Copia ( es archivo se copia en Server2\Compartida2\Sistemas2\Copias20XX\ Xxx20XX que corresponde al mes y al año ej Ene2020..despues \Corr\copiaddmmaaaa ej: Copia27Ene2020 y equipo de VentanillaÚnica (\\VENTANILLA\Ventanilla\_unica\_año actual\CORRESPONDENCIA RECIBIDA.xls y \\VENTANILLA\Ventanilla\_unica\_año actual\CORRESPONDENCIA ENVIADA del mes y día correspondiente, \\VENTANILLA\Ventanilla\_unica\_año actual\CORRESPONDENCIA RECIBIDA del mes y día correspondiente.

Este procedimiento será realizado por el personal de TIC del INVISBU.

### COPIAS DE SEGURIDAD PERIODICA

Se harán copias mensuales en el servidor, equipo de sistemas, en el hosting dos por mes y en un disco externo; de los siguientes archivos, así:

**Procedimiento:** Se hará copia de la carpeta comprimida del mes a copiar en el disco del hosting de INVISBU Aquí se debe incluir Archivos de correspondencia hoja Excel, Correspondencia Enviada y Revida, Eco

**PLAN DE COPIAS DE SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO DEL INVISBU**

Financiero, Archivos de Propiedad Horizontal, Archivo de Nomina que se encuentra en el GD ( estará a cargo del administrador del aplicativo GD y del usuario del sistema) y Archivos de la Pagina Web que se encuentran en el área del Hosting; Este archivo debe quedar copiado en Server2\Compartida2\Sistemas2\Copias 20XX (XX será el correspondiente al año en curso); para hacer la copia se entra al sitio "invisbu/private/copias\_seguridad" con el FileZilla Client. De esta copia se deberán mantener los dos últimos archivos como mínimo.

- Archivos Sistema ECO está ubicado en el servidor en la nube y las copias de seguridad están a cargo del proveedor del Servicio. (Se le pedirá al proveedor del servicio copia mensual de las bd del sistema)

Este procedimiento será realizado por el personal de TIC del INVISBU.

El proceso de copias de seguridad de los equipos debe ser realizado de acuerdo al cronograma que a continuación se anexa teniendo en cuenta las fechas establecidas en el presente plan y será previamente comunicado a los usuarios.

**CRONOGRAMA**

**COPIA DE SEGURIDAD  
 EJECUCIÓN DE ENERO A DICIEMBRE AÑO 2023**

	<b>NOMBRE DISPOSITIVO</b>	<b>USUARIO/DEPENDENCIA</b>	<b>Nro. INVENTARIO</b>	<b>DIA_MES</b>
1	SISTEMAS01	Javier Orlando Nuñez/TIC	0651	16_Mar
2	SISTEMAS05	Silvia Hernández/TIC	0652	16_Mar
3	SISTEMAS08	Marcia Solano Álvarez/TIC	0789	23_Mar
4	Portatil1	Javier Orlando Nuñez /TIC	0443	23_Mar
5	Portatil2	Javier Orlando Nuñez /TIC	0438	23_Mar
6	DIRECCION	No está en uso/Dirección	0439	24_Mar
7	SECTECNICA21	Patricia Durán/Técnica	0834	30_Mar
8	TECNICA11	Marjhen Durán/Técnica	0771	13_Abr
9	TECNICA17	Claudia Murcia/Técnica	0770	20_Abr
10	TECNICA18	Carlos Santamaria/Técnica	0772	27_Abr
11	TECNICA21	Erika Díaz/Técnica	0773	04_May
12	ProfesionalTec2	Jorge Eduardo Gutiérrez/Técnica	0738	11_May
13	TECNICA4	Debajo escritorio-No uso/Técnica	0624	11_May
14	JURIDICADIR	Adneris Amorocho/Dirección	0833	18_May
15	SUBJURIDICA	Xiomara Ortiz/Jurídica	0832	25_May
16	ASEJURIDICO	Mónica Suarez/Jurídica	0769	01_Jun
17	JURIDICA15	Wilmer Zafra/Jurídica	0780	08_Jun
18	Juridica14	Juliana Barragán/Jurídica	0781	15_Jun
19	JURIDICA13	Myriam Chavarro/Jurídica	0782	22_Jun
20	PROPIEDADHO1	Juan Pablo Barrero/Jurídica	0460	29_Jun
21	PROPIEDADHO2	Jenny Marcela Suarez/Jurídica	0526	06_Jul
22	JURIDICA05	Carolina Cruz/Jurídica	0264	20_Jul
23	JURIDICA012	Karen Viviana Casanova/Jurídica	0437	27_Jul
24	Juridica5	Carolina Cruz/Jurídica	0459	03_Ago
25	DESKTOP-U1HHVD9	Claudia Mendoza/Tesorería	0627	10_Ago

**PLAN DE COPIAS DE SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO DEL INVISBU**

26	adminplan01	Claudia Mendoza/Tesorería	0453	10_Ago
27	PORTATIL5	Maritza Gómez/Contabilidad	0442	17_Ago
28	ADMIN-CONTA04	Maritza Gómez/Contabilidad	0633	17_Ago
29	CONTABILIDAD03	Julieth Garavito/Contabilidad	0775	24_Ago
30	presupuesto	María Inés/Presupuesto	0630	31_Ago
31	ALMACEN	Jorge Saavedra/Almacén	0629	07_Sep
32	ventanilla	Luz Marina Gálvez/Ventanilla	0454	08_Sep
33	ARVHIVO05	Fabiola Trillos/Archivo	0195	14_Sep
34	juridica08ph	Nancy Rodríguez/Archivo	0261	21_Sep
35	ARVHIVO04	Carlos Amaya/Archivo	0835	28_Sep
36	ARVHIVO05	Marlon García/Archivo	0794	05_Oct
37	DESKTOP-DIEGO	Diego Amaya/Sub. Administrativa	0194	12_Oct
38	SECADTIVA	Laura Suarez/ Sub. Administrativa	0452	19_Oct
39	SUBADTIVA	Alexandra/Sub. Administrativa	0436	26_Oct
40	Lester	Lester Cuellar/Control Interno	0256	02_Nov
41	DESKTOP-KNPU795	Oscar Flórez/Control Interno	0707	09_Nov
42	CONTROLINTERNO01	Jorge Vargas/Control Interno	0779	16_Nov
43	planeacion01	Asesor (Carolina)/Planeación	0783	23_Nov
44	PORTATIL6	Carolina/Planeación	0441	23_Nov
45	subdioperativa	Nelson Guerrero/Operativa	0778	30_Nov
46	DESKTOP-J7GJ22L	Judith C. Sánchez/Operativa	0455	01_Dic
47	juridica07ph	Contratistas/Operativa	0435	07_Dic
48	OPERATIVA02	Claudio Meneses/Operativa	0193	14_Dic
49	PORTATIL3		0282	15_Dic
50	PORTATIL4	Bodega	0197	15_Dic

**RECOMENDACIONES**

Se deberá brindar el servicio de copias de seguridad de emergencia ante un desperfecto presentado en cualquier equipo del instituto, para este servicio se requerirá realizar una solicitud al asesor de sistemas.

El personal técnico apoyará en las actividades programadas para las copias de seguridad del INVISBU.

Una vez terminada la parte técnica de la copia de Seguridad, el personal responsable, realizará recomendaciones a cada uno de los usuarios, con el objetivo de que estos contribuyan con la conservación de la información. Las recomendaciones que se socializarán serán las siguientes:

- No apagar el equipo, sin antes salir adecuadamente del sistema
- Realizar respaldos de información crítica periódicamente
- Tener en cuenta que solo se hará copia de la información institucional ubicada en la carpeta de backup.
- La copia de seguridad se realizara el mismo día del mantenimiento preventivo
- Consultar con el personal de redes o cómputo cualquier duda o situación que se Presente con el equipo de cómputo. Llamar a la extensión sistemas 121.

**PLAN DE COPIAS DE SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO DEL INVISBU**

Elaboro,  
**Ing. JAVIER ORLANDO NÚÑEZ LATORRE**  
Asesor TIC