

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

FECHA (11/04/2024)

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 Institucionales, 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 Institucionales 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 PERIODICO (quincenal)

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: E:\CopiasCorr20XX\Copia (es archivo se copia en Server2\Compartida2\Copias20XX\Mes ejr\Corr\copiaDDmmm20XX que corresponde al Dia, Mes y al año ej. Copia15Abr2024 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 periódicamente 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 pueden incluir Archivos de correspondencia hoja Excel, Correspondencia Enviada y Recibida, Eco 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

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

en el área del Hosting; Este archivo debe quedar copiado en Server2\Compartida2\Copias 20XX (XX será el correspondiente al año en curso); para hacer la copia se entra al sitio "invisbu/private/copias_seguridad" con el Cpanel. 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 ABRIL A DICIEMBRE AÑO 2024**

	NOMBRE USUARIO WINDOWS	USUARIO/DEPENDENCIA	Nro. INVENTARIO	DIA_MES
1	SISTEMAS01\admin	Asesor TIC	0651	16_Abr
2	sistemas	Asesor TIC	0652	18_Abr
3	TIC1	Asesor TIC	0789	23_Abr
4	DIRECCION INVISBU	Asesor TIC	0439	25_Abr
5	Portatil1 ACER	Asesor TIC	0443	30 Abr
6	Portatil2 LENOVO	Asesor TIC	0438	2 May
7	TECNICA21	Subdireccion Técnica	0773	7 May
8	SECTECNICA	Secretaria Técnica	0834	9 May
9	ProfesionalTec2	Profesional Técnica	0738	14 May
10	TECNICA17	Contratista1 Técnica	0770	16 May
11	TECNICA11	Contratista2 Técnica	0771	21 May
12	User	Contratista3 Técnica	0772	23 May
13	Secretaria Direccion	Secretaria Direccion1	0833	28 May
14	JURIDICA14	Secretaria Direccion2	0781	30 May
15	Subdireccion Juridica	Subdireccion Jurídica	0832	4 Jun
16	JURIDICA13	Secretaria Jurídica	0782	6 Jun
17	Asesor_Juridico	Asesor Jurídico	0769	11 Jun
18	SISTEMAS10	Profesional Propiedad H	0460	13 Jun
19	ADNERYS AMOROCHO	Contratista1 Jurídica	0526	18 Jun
20	Juridica02	Contratista2 Jurídica	0780	20 Jun
21	JURIDICA012	Contratista3 Jurídica	0437	25 Jun
22	JURIDICA	Contratista4 Jurídica	0264	27 Jun
23	VENTANILLA\ventanilla1	Ventanilla	0905	2 Jul
24	Fabiola Trillos	Auxiliar1 Archivo	0195	4 Jul
25	CARLOS AMAYA	Auxiliar2 Archivo	0835	9 Jul
26	ARCHIVO05	Contratista1 Archivo	0794	11 Jul
27	JURIDICA08PH\Archivo 02	Contratista2 Archivo	0261	16 Jul
28	ALMACEN	Almacén	0624	18 Jul
29	SUBDIRECCION ADTIVA	Subdirección Administrativa	0436	23 Jul
30	TESORERIA	Tesoreria1	0627	25 Jul

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

31	ADMINPLAN01\Tesoreria	Tesoreria2	0453	30 Jul
32	CONTABILIDAD	Contabilidad1	0633	1 Ago
33	Portatil3	Contabilidad2 Portátil	0442	6 Ago
34	AUXILIAR01	Auxiliar Administrativo1	0775	8 Ago
35	Diego	Auxiliar Administrativo2	0194	13 Ago
36	Admin09	Secretaria Administrativa	0452	15 Ago
37	INVISBU\admin_presupuesto03	Presupuesto	0630	20 Ago
38	Control Interno	Jefe de Control interno	0779	22 Ago
39	CONTROL INTERNO	Contratista1 Control Interno	0707	27 Ago
40	Lester	Contratista1 Control Interno	0256	29 Ago
41	OPERATIVA09	Subdireccion Operativa	0778	3 Sep
42	secretariaoperativa	Secretaria Operativa	0455	5 Sep
43	Operativa	Profesional Operativa	0193	10 Sep
44	INVISBU\juridica07ph	Contratista1 Operativa	0435	12 Sep
45	Juridica03	Contratista2 Operativa	0459	17 Sep
46	Portatil4	Portátil1 Operativa	0282	19 Sep
47	Portatil5	Portátil	0441	24 Sep
48	PLAN	Asesor Planeación	0783	26 Sep
49	Portatil6	Portatil1 Bodega	0197	1 Oct

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.

Elaboro,
Ing. JAVIER ORLANDO NÚÑEZ LATORRE
 Asesor TIC