NOMBRE DEL PROCEDIMIENTO: Tratamiento y Resguardo de Información de Servidores Institucionales

CÓDIGO DEL PROCEDIMIENTO: 64-DPF-P16/Rev.03 **FECHA DE EMISIÓN:** 26/05/2016

I.- OBJETIVO DEL PROCEDIMIENTO

Mantener la integridad la información y equipo, que está bajo resguardo de la Subdirección de Sistemas y Tecnologías que depende de la Dirección de Planeación y Finanzas de DIF Sonora..

II.- ALCANCE

Estos procedimientos aplican a la Subdirección de Sistemas y Tecnologías para el resguardo de la integridad física de la información crítica que se encuentra en los servidores de datos (a excepción del correo), para evitar una contingencia que se constituya en una fuga y /o pérdida de información por una falla técnica. La efectividad del procedimiento está sujeta a la capacidad del hardware que se dispone para llevar a cabo dicho procedimiento.

III.- DEFINICIONES

1. Hardware: corresponde a todas las partes físicas y tangibles de una computadora.
2. Software: los componentes intangibles de una computadora. Conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea.
3. Usuario: individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático en la Institución.
4. Sistema solicitudes de soporte: sistema donde se capturan las solicitudes de servicio de los programas de la Institución.
5. Sistema: programa desarrollado en un lenguaje informático destinado a una función específica.
6. Características del servicio: Oportuno, eficiente, efectivo, tanto en su aspecto preventivo como en el correctivo, además, amable en caso de interactuar con el personal relacionado con el servicio.
7. S.O., SO/ s.o.,so: sistema operativo.
8. Servidor o server: se denomina servidor a todo aquel equipo de altas prestaciones, que ha sido diseñado y asignado a tareas de compartir información, servicios y/o particiones para alguna tarea.
9. Virtualización: técnica mediante la cual un equipo de altas prestaciones, regularmente un servidor se utiliza para emular la existencia física de 2 o más servidores.
10. Visor de sucesos: herramienta que forma parte del conjunto de herramientas de administración de servidores Micro Soft y se refleja el estado del servidor en general.
11. Base de datos: conjunto de tablas y archivos fichas o ficheros que están relacionados y organizados de manera lógica para contener la información.
12. M.S. /MS : micro soft
13. Firewall: equipo dedicado al filtrado y administración de tráfico entre la red LAN y la red Wan.
14. LAN: red de área local.
15. Wan : red de área extendida (Entiéndase red de redes aunque también se usa para referirse al Internet)

IV.- REFERENCIAS

1. Reglamento Interior del Sistema para el Desarrollo Integral de la Familia del estado de Sonora.
2. Acuerdo por el que se establecen las Disposiciones en materia de control interno para la Administración Pública Estatal.
3. Cualquier disponible en internet, buscador de internet en general y en soporte técnico Microsoft en la página web empezando por http://support.microsoft.com/AllProducts. En caso de haberlo se consulta o se turna con un consultor externo que asesore al área de sistemas.
4. 64-DPF-P14 Solicitud de Soporte de Sistemas.

V.- POLITICAS

1. Antes de implementar un nuevo servidor se debe de analizar, si el equipo es capaz de satisfacer la necesidad o se requiere uno nuevo.
2. Es necesario determinar los servicios que proveerá el servidor para implementar el uso adecuado.
3. Cada servidor deberá contar con un antivirus, anti-spyware.
4. Se debe instalar software de librerías y programas utilitarios requeridos para el cumplimiento del servicio para el que fue implementado.
5. La supervisión de los servidores se debe hacer diariamente, para conocer su estado de servicio, se debe asignar una persona responsable de esta tarea y en ausencia uno de los administradores lo hará en su lugar.
6. Los servidores deben quedar incluidos en el segmento de red definido para este tipo de equipos.
7. La segmentación de la red está sujeta a la capacidad técnica disponible.
8. Los servidores deben estar protegidos por firewall.
9. En caso de que el servidor aloje información sensible y crítica, se deben tomar las medidas para asegurarse de que dicha información sea debidamente respaldada y resguardada.
10. Los servidores son físicos o virtuales esto dependerá del criterio del administrador para evaluar prestaciones y o demanda de servicio.
11. Para definir qué información se respalda se tomara en cuenta lo critico de la información y la capacidad técnica disponible.
12. Los servidores deben permanecer encendidos y en operación durante la ejecución del respaldo.
13. Ningún servidor debe ser reiniciado o apagado sin notificar debidamente al área de redes de DIF Sonora.
14. Solo se respaldaran los servidores que sean considerados críticos para la operación de DIF Sonora.
15. Los riesgos en el servicio de Redes y Seguridad en la información que se prevén con este procedimiento son, pérdida de información por fallas técnicas, hacking internos o externos y virus.
16. Se considera un espacio restringido para proteger la información institucional el espacio que ocupa Site de servidores.

VI.- FORMATOS E INSTRUCTIVOS

Clave de Formato/Instructivo	Nombre del Formato/Instructivo
64-DPF-P16-F01/Rev.03	Registro de chequeo de servidores.

VII.- ANEXOS

Clave de Anexo	Nombre
64-DPF-P16-A01/Rev.03	Diagrama de flujo del procedimiento de Tratamiento y resguardo de información se servidores institucionales

VIII.- DESCRIPCIÓN DE LA OPERACIÓN DEL PROCEDIMIENTO			
NO	RESPONSABLE	DESCRIPCIÓN DE ACTIVIDADES	REGISTRO
1		SUPERVISIÓN DEL ESTADO DE LOS SERVIDORES MEDIANTE REVISIÓN DEL VISOR DE SUCESOS.	
1.1	Coordinador de Redes y Seguridad en la Información	Inicia una sesión remota o directamente en cada uno de los servidores.	
1.2		Entra en el visor de sucesos para su revisión.	
		"Si detecta errores"	
1.3		Registra errores en el sistema de solicitudes de soporte de servidores poniendo especial atención a los mensajes de advertencia y errores. (warnings y error) y/o registro de estado de servidores.	Registro de chequeo de servidores 64-DPF-P16-F01
1.4		Inicia búsqueda en internet con el tema del error y si es (en x servidor de búsqueda) o se busca soporte en la página web de Microsoft http://support.microsoft.com/AllProducts y si se cuenta con el recurso el asesor contratado para sistemas.	
1.5		Soluciona los errores tomando las medidas correctivas o preventivas, dependiendo el tipo de error y advertencia encontrada.	
1.6		Registra resultados obtenidos, en sistema de solicitud de soporte y registro de chequeo de servidores.	Registro de chequeo de servidores 64-DPF-P16-F01
		"Si todo se encuentra normal"	
1.7		Cierra el visor de sucesos y conexión remota.	
2		PROTECCIÓN ANTI-VIRUS Y ANTI-SPYWARE DE SERVIDORES INSTITUCIONALES.	
2.1	Coordinador de Redes y Seguridad en la Información	Inicia sesión remota o directamente en cada uno de los servidores.	
2.2		Abre una instancia del software antivirus y verifica la vigencia del software y del catálogo de virus.	
2.3		Revisa el último escaneo antivirus de archivos.	
		"Si el último escaneo tiene más de 7 días "	

2.4		Activa escaneo antivirus de forma manual y registra en sistema de solicitudes de soporte y registro de chequeo de servidores.	Registro de chequeo de servidores 64-DPF-P16-F01
		"Cuando se detectan virus"	
2.5		Verifica que se haya puesto en cuarentena, establece acciones para erradicar el virus y registra.	Registro de chequeo de servidores 64-DPF-P16-F01
2.6		Cierra la instancia del software A.V. al terminar la tarea.	
2.7		Cierra la sesión del servidor al término del procedimiento de protección antivirus.	
3		VERIFICACIÓN DEL ESTADO DE LA RED POR MEDIO DE HERRAMIENTA VISUAL.	
3.1	Coordinador de Redes y Seguridad en la Información	Ingresa a navegador y verifica tablero de control de servidores.	
		" Si se detectan fallas"	
3.2		Detecta los equipos que presentan fallas de comunicación.	
3.3		Verifica si la falla es real o es un falso positivo.	
		"Si es real"	
3.4		Detecta si el servidor está apagado o colapso y toma las medidas correctivas.	
3.5		Registra las acciones realizadas en sistema de solicitud de soporte y registro de chequeo de servidores.	Registro de chequeo de servidores 64-DPF-P16-F01
4		VERIFICACIÓN DE LOS REPORTES DE FALLA DE CONEXIÓN.	
4.1	Coordinador de Redes y Seguridad en la Información	Verifica si existen reportes de falla de conexión hecho por usuarios por medio del sistema de soporte.	
4.2		Verifica la herramienta visual en caso de no haber falla, verifica si el servidor responde correctamente a una petición de servicio (conexión).	
4.3		Verifica el reporte con el usuario.	
		"Si el problema no es en la red y se trata de un problema aislado y único del usuario que lo reporta"	
4.4		Canaliza el reporte al área de soporte para que lo atienda como falla del equipo.	
4.5		Registra actividades realizadas en sistema de solicitud de soporte y/o registro de chequeo estado de servidores	Registro de chequeo de servidores 64-DPF-P16-F01

5		ADMINISTRACIÓN DE ROUTER QUE JUNTA EL TRÁFICO DE LAS DIFERENTES REDES DE DIF SONORA HACIA LOS SERVIDORES.	
5.1	Coordinador de Redes y Seguridad en la Información	Ingresa al router mediante herramienta de administración web.	
5.2		Controla el acceso de los equipos a la red en el router.	
5.3		Asigna dirección IP, de acuerdo a router de dirección IP.	
5.4		Monitorea tráfico de datos por la red y ruteo.	
5.5		Ajusta el ruteo según necesidades de servicio cada vez que se requiera.	
5.6		Respalda de la configuración cada que hay una modificación.	
5.7		Registra las actividades realizadas, en sistema de solicitudes de soporte y registro de chequeo estado de servidores.	Registro de chequeo de servidores 64-DPF-P16-F01
6		ADMINISTRACIÓN DE FILTROS DE CONTENIDO (PROXY) DE DIF SONORA	
6.1	Coordinador de Redes y Seguridad en la Información	Entra al Proxy mediante una herramienta de administración web para la administración de filtros de contenido.	
6.2		Ajusta para el bloqueo de sitios sospechosos y de virus de acuerdo a las necesidades institucionales.	
6.3		Controla los servicios de red y accesos del exterior de acuerdo con las con las necesidades institucionales.	
6.4		Respalda últimas configuraciones al final de cada modificación.	
6.5		Registra resultados en sistema de solicitud de soporte y registro de chequeo estado de servidores	Registro de chequeo de servidores 64-DPF-P16-F01
7		RESPALDO DE LA INFORMACIÓN CRITICA DE LOS SERVIDORES DE DIF SONORA.	
7.1	Coordinador de Redes y Seguridad en la Información	Abre sesión remota o directamente en el servidor.	
7.2		Entra al programa designado para el respaldo.	
7.3		Verifica la disponibilidad de acceso de la información a respaldar en el servidor.	

7.4		Entra en la programación de respaldos e inscribe los nuevos datos para que se incluyan en el próximo respaldo.	
7.5		Guarda configuración y cierra programa de respaldo.	
7.6		Termina la sesión remota y registra resultados en sistema de solicitudes de soporte y/o registro de chequeo estado de servidores	Registro de chequeo de servidores 64-DPF-P16-F01
8		VERIFICACIÓN DE RESPALDOS.	
8.1	Coordinador de Redes y Seguridad en la Información	Inicia una sesión remota o directamente en el servidor.	
8.2		Verifica la fecha del último respaldo y el espacio disponible.	
		"Si el respaldo no se hizo o si falta espacio"	
8.3		Toma las medidas correctivas necesarias para que se haga el respaldo.	
		"Si todo está bien."	
8.4		Cierra el software de respaldo.	
8.5		Termina sesión remota.	
8.6	Coordinador de Redes y Seguridad en la Información	Registra resultado en sistema de solicitud de soporte y registro de chequeo estado de servidores.	Registro de chequeo de servidores 64-DPF-P16-F01
		"Una vez al año o cuando ingresa personal al Área"	
8.7	Coordinador de Redes y Seguridad en la Información	Da a conocer al personal que labora en la coordinación: la misión, visión, valores, manual de organización, objetivo, funciones, facultades, metas y actividades para cumplirlas, indicadores, procedimientos y registros, así como las reglas de operación existentes, realiza los entrenamientos que se requieran y registra en minuta.	Minuta 64-DGD-P01-F01
8.8		Realiza verificación a la ejecución del proceso de manera semestral.	
		"Si detecta desviaciones"	
8.9		Realiza correcciones y registra en minuta.	Minuta 64-DGD-P01-F01
FIN DEL PROCEDIMIENTO			

Elaboró: **Revisó:** **Aprobó:**

C. Fabián Silva Dórame/ Coordinador de Redes y Seguridad en la Información.	Lic. Julio Cesar Vidaña García/ Subdirector de Sistemas y Tecnología	Lic. José Agustín Pacheco Tapia/ Director de Planeación y Finanzas