Municipalidad Metropolitana de Lima

INVERMET | FONDO METROPOLITANO DE INVERSIONES

RESOLUCION Nº191 -2015-INVERMET-SGP

Lima, 12 JUN 2015

VISTO:

El Informe N° 057-2015-INVERMET-OPP de la Oficina de Planificación y Presupuesto y el Informe Nº 016-2015-INVERMET/OPP/INF del Área de Informática;

CONSIDERANDO:

Que, INVERMET es una entidad pública creada por el Decreto Ley N° 22830 de fecha 26 de diciembre de 1979, con el objeto de proporcionar recursos para el programa de obras de la Municipalidad Metropolitana de Lima, habiéndose aprobado su Reglamento con el Acuerdo N° 083 de fecha 03 de setiembre de 1996, del Concejo Metropolitano de Lima, constituyéndose como un Organismo Público Descentralizado de la Municipalidad Metropolitana de Lima, con personería jurídica y autonomía administrativa económica y técnica;

Que, el Área de Informática, a través del Informe N° 016-2015-INVERMET-OPP/APP de fecha 07 de abril del 2015, procedió a elaborar el proyecto de directiva denominado "Procedimientos de Ejecución de Copias de Respaldo Y Protección Antivirus en el Fondo Metropolitano de Inversiones - INVERMET", la misma que tiene por finalidad, establecer los procedimientos de ejecución y manejo adecuado de las copias de respaldo "Backup" y para la protección de la información almacenada en archivos digitales contra los ataques de virus informáticos y/o manipulaciones indebidas a fin de dar respuesta oportuna, adecuada y coordinada, ante cualquier contingencia, deberán ser conservadas fuera de las instalaciones del local institucional;

Que, al haberse cumplido con las formalidades y procedimientos establecidos en la Directiva N° 010-INVERMET/SGP "Directiva General para la Formulación, Modificación y Aprobación de Directivas del Fondo Metropolitano de Inversiones – INVERMET", corresponde dictar el acto de administración que apruebe el proyecto de Directiva denominado "Procedimientos de Ejecución de Copias de Respaldo Y Protección Antivirus en el Fondo Metropolitano de Inversiones - INVERMET", para lo cual debe dictar la correspondiente resolución del titular de la entidad;

Con el visado de la Oficina de Planificación y Presupuesto y de la Oficina de Asesoría Jurídica;

En uso de las atribuciones conferidas por los artículos 19 y 20 del Reglamento del Fondo Metropolitano de Inversiones - INVERMET, aprobado por el Acuerdo de Concejo N° 083 de fecha 03 de setiembre de 1996;

Municipalidad Metropolitana de Lima

INVERMET | FONDO METROPOLITANO DE INVERSIONES

SE RESUELVE:

Artículo Primero.- Aprobar la Directiva N° 001-2015-INVERMET-SGP denominada "Procedimientos de Ejecución de Copias de Respaldo Y Protección Antivirus en el Fondo Metropolitano de Inversiones - INVERMET".

Artículo Segundo.- Notificar la presente Resolución a las diferentes dependencias de la entidad, para su conocimiento y fines.

Artículo Tercero.- Encargar al responsable del Portal de Transparencia de la Institución efectúe la publicación de la presente Resolución y la correspondiente Directiva en el portal Institucional www.invemet.gob.pe.

Regístrese y Comuníquese

MUNICIPALIDAD METROPOLITANA DE LIMA
Fondo Metropolitano de Inversiones INVERMET

Ing. LUIS ANTONIO ROBLES RECAVARREN
Secretario General Permanente

Municipalidad Metropolitana de Lima

INVERMET FONDO METROPOLITANO DE INVERSIONES

MUNICIPALIDAD METROPOLITANA DE LIMA

FONDO METROPOLITANO DE INVERSIONES INVERMET

DIRECTIVA N° 001-2015-INVERMET-SGP "PROCEDIMIENTO DE EJECUCIÓN DE COPIAS DE RESPALDO Y PROTECCIÓN ANTIVIRUS"

DIRECTIVA N° 001-2015-INVERMET-SGP

PROCEDIMIENTO DE EJECUCIÓN DE COPIAS DE RESPALDO Y PROTECCIÓN ANTIVIRUS

I. OBJETIVOS

1.1 Establecer el procedimiento para la ejecución y manejo adecuado de las copias de respaldo "Backup" de la información del Fondo Metropolitano de Inversiones - INVERMET en archivos digitales, con el fin de asegurar su conservación e integridad.

1.2 Establecer el procedimiento para la protección de la información almacenada en archivos digitales, contra los ataques de virus informáticos y/o manipulaciones indebidas, previniendo la presencia de software malicioso en el computador tecnológico del Fondo Metropolitano de Inversiones - INVERMET y proceder a su eliminación una vez detectados.

II. FINALIDAD

Se busca establecer los procedimientos internos que debe seguir la Entidad, para asegurar la conservación e integridad de la información almacenada en los sistemas aplicativos de INVERMET, a través de una oportuna, adecuada y coordinada, copia de respaldo "Backup".

III. BASE LEGAL

3.1 Decreto Ley N° 22830 - que crea el Fondo Metropolitano de inversiones-INVERMET, sus modificatorias, ampliatorias y conexas.

3.2 Acuerdo de Concejo N° 083 - Reglamento del Fondo Metropolitano de Inversiones - INVERMET.

3. 3 Ley N° 27245- Ley Responsabilidad y Transparencia Fiscal y Modificatorias

3.4 Ley N° 27658 - Ley Marco de Modernización de la Gestión del Estado.

3.5 TUO de la Ley N° 27806 - Ley de Transparencia y Acceso a la Información Pública, aprobado con Decreto Supremo N°043-2003-PCM y modificatorias.

3.6 Ley N° 27815 - Ley del Código de Ética de la Función Pública sus Modificatorias y Reglamento aprobado con D. S. N° 033-2005-PCM.

3.7 Ley N° 27952- Ley Orgánica de Municipalidades.

3.8 Ley N° 28411 - Ley General del Sistema Nacional de Presupuesto.

3.9 Ley N° 28716 - Ley de Control Interno de las Entidades del Estado.

3.10 Resolución de Contraloría N° 320-2006-CG

3.11 Acuerdo del Comité Directivo N° 821-1 y Resolución N° 009-2011-CD, aprueban el Reglamento de Organización y Funciones- ROF del INVERMET.

3.13 Acuerdo del Comité Directivo N° 835-2 - aprueba el Manual de Organización y Funciones - MOF del INVERMET.

3.14 Resolución Ministerial N° 129-2012-PCM aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 EDI Tecnología de la Información.

IV. ALCANCE

La presente directiva es de aplicación obligatoria a todos los archivos generados del Sistema Integrado de Gestión de INVERMET.

V. VIGENCIA

La presente directiva entra en vigencia a partir del día siguiente de su aprobación y difusión.

VI. DISPOSICIONES GENERALES

El procedimiento se aplica en los siguientes ambientes tecnológicos:

a) Servidores que hace parte de la plataforma Tecnológica de INVERMET.

b) Todas las computadoras de escritorio, portátiles conectados a la plataforma tecnológica de INVERMET.

VII. DISPOSICIONES ESPECÍFICAS

7.1 Operación de copias de respaldo

Identificado el número de aplicativos y/o base de datos para el respaldo, determinando los mecanismos según la base de datos a respaldar: manual o automático.

7.2 El Operador de Backup (OB)

7.2.1 Ejecuta copias de respaldo en los tapes, en la que almacena toda la información archivada de las carpetas del servidor de INVERMET, base de datos, archivos del servidor y otros.

7.2.2 Archiva la cinta que se utilizó para el Backup diario hasta el día jueves y la cinta Backup con copia de respaldo del día viernes.

7.2.3 Ejecuta y archiva el Backup mensual el último día laborable del mes, debiendo identificar las cintas según la codificación asignada (Tabla *N°01).*

Tabla N° 01: CODIFICACIÓN DE CINTA DE BACKUP

FRECUENCIA	TIPO DE BUCKUP	DISPOSITIVO DE ALMACENAMIENTO	IDENTIFICACION DE LA CINTA BACKUP	INFORMACION RESPALDADA DE CINTAS	
				SERVIDOR QUE REALIZA BACKUP	CONTENIDO
Diario	Full Backup	Cinta nueva	DD/MM/YYY-SXX-F	SL1 FILE001	Backup de todas las carpetas de usuarios de los servidores TIERRA, SL1FILE001, SERVER SEERVERBD Y SVRDC01
Semanal	Full Backup	Cinta nueva	DD/MM/YYYY-SXX-FS	SL1FILE002	Backup de todas las carpetas de usuario de los servidores TIERRA. SL1FILE001, SERVER, SERVERBD Y SVRDC02
Mensual	Full Backup	Cinta Nueva	DD/MM/YYY-MXX	SL1FILE003	Backup de todas las carpetas de usuario de los servidores TIERRA, SL1FILE001, SERVER, SERVEREBD Y SVRDC03

Dónde:

- DD: Día (01, 02, 03,.....)
- MM: Mes (01, 02, 03,.....)
- YYYY: Año (2014, 2015, 2016,.....)
- SXX: Semana (01, 02, 03,.....)
- MXX: Mes (01, 02, 03,.....)
- F: Cinta de lunes a jueves
- FS: Cinta del Viernes.

7.2.4 Verifica el resultado de las copias de respaldo, en caso de presentar fallas durante su ejecución, se debe identificar sus causas con el fin de dar solución al inconveniente y volver a ejecutar la actividad que realiza al Backup o copia afectada.

7.2.5 Procede a ejecutar copias de respaldo no programadas en caso crea conveniente, asimismo solicita la segunda copia de respaldo al responsable de su custodia en caso de desastres (terremoto, incendio, etc.), copia que por lo general se encuentra ubicada en un lugar seguro fuera de las instalaciones de INVERMET.

7.3 Restauración de información de copias de respaldo

Los colaboradores para solicitar la recuperación de copias de respaldo de los archivos perdidos del servidor, deberán comunicar vía correo electrónico (con copia al Jefe inmediato) a la oficina de sistemas, especificando lo siguiente:

- Fecha de pérdida.
- Nombre del archivo.
- Tipo de documento.
- Ruta de identificación.

7.4 Almacenamiento

7.4.1 A fin de proteger la integridad de la información de los servidores TIERRA, SL1FILE001, SERVER, SERVERBD y SVRDC01, se mantiene en un ambiente cerrado debidamente ventilado y con acceso restringido en la oficina de sistemas.

7.4.2 Una copia de las cintas de Backup mensual del servidor TIERRA, SL1 FILE001, SERVER, SERVERBD y SVRDC01, son conservadas fuera de las instalaciones de INVERMET, ante cualquier contingencia (oficinas de resguardo).

7.4.3 Se mantienen cintas con las copias de respaldo de los servidores por los siguientes periodos:

- Backup diario: de los últimos cinco (05) días laborables de la semana.
- Backup semanal: de los últimos seis (06) meses.
- Backup mensual: de los últimos veinticuatro (24) meses.

7.5 Protección antivirus

El Área de Informática o quien haga sus veces, de la Oficina de Planificación y Presupuesto, debe instalar un software antivirus en todos los servidores, PC"s con acceso a internet, USB y CD-ROM, actualizando vía internet del site del fabricante, en forma diaria y/o semanalmente (Tabla N° 02).

Tabla N° 02

N°	ACTIVIDAD	RESPONSABLE
1	Configurar la consola del antivirus en el servidor, de acuerdo a los parámetros definidos por el Ingeniero de Seguridad en lo referente a "configuración de antivirus".	Soporte Informático
2	Verificar las formas del antivirus en los computadores, los cuales deben ser actualizados todos los días. En caso que se detecten firmas desactualizadas, proceder con la descarga de manera manual desde el portal fabricante del Antivirus utilizado.	Soporte Informático
3	La consola del antivirus debe estar con acceso a internet! para la actualización de las firmas del antivirus es automático.	Soporte Informático
4	Verificar el reporte de actualización generado por la consola del antivirus, donde se presentan los porcentajes de actualización con la respectiva versión, así como el número de equipos con antivirus.	Soporte Informático
5	Ejecutar el Plan de Acción con el fin de dar solución a los casos más críticos en la actualización de los equipos.	Coordinador de Informática Especialista de Redes y Comunicaciones Soporte
6	Llegar al sitio y tomar control del equipo e informar al usuario las acciones que se van a realizar, además de desconectarlo de la red o cualquier otra acción que considere necesaria.	Soporte Informático
7	Verificar la versión del antivirus que tiene el usuario instalado en ese momento, si tiene la última versión disponible.	Soporte Informático
8	Actualizar el software de antivirus a la última versión disponible. Esta actualización debe realizarse desde la consola del antivirus o si se requiere localmente.	Soporte Informático
9	Ejecutar el software del antivirus, para que haga la limpieza automática a todos los discos duros del equipo.	Soporte Informático

OFICINA DE PLANIFICACIÓN Y PRESUPUESTO INVERMET V°B° J.V.B.

7.6 El Operador de Backup (OB)

7.6.1 Remite comunicados a todas las dependencias de INVERMET, alertando sobre nuevos virus, realizando revisiones diarias de los servidores y PC's para descartar virus o cualquier otro tipo de amenaza, debiendo verificar que se hayan ejecutado todas las actualizaciones requeridas.

AREA DE INFORMATICA INVERMET V°B° L.A.R.C.

7.6.2 Al identificar un virus o anormalidades en los servidores o PC's, se procede a evaluar el daño en el software y restaurar la información contenida en las copias de respaldo o reinstalar el software de ser necesario, registrando la información más resaltante.

VIII. RESPONSABILIDADES

8.1 Jefe de la Oficina de Planificación y Presupuesto

Es el responsable de asegurar el cumplimiento de la presente directiva.

8.2 Coordinador de Informática

Es el responsable de verificar el cumplimiento de la presente directiva y de ejecutar el plan de acción con el fin de dar solución a los casos más críticos en la actualización de equipos.

8.3 Operador de Backup

Es el responsable de realizar las copias de seguridad.

8.4 Servidores de cualquier modalidad de contrato

Son responsables de guardar su información más importante en las carpetas que tienen asignadas en el servidor de archivos.

8.5 Especialista de redes y comunicaciones

Participa en las modificaciones del procedimiento, así como en la definición del estándar para la configuración de antivirus.

8.6 Soporte Informático

Define, instala y mantiene actualizado el software de antivirus. Establece e implanta un plan de acción para eliminar los virus que el antivirus no ha podido eliminar.

OFICINA DE PLANIFICACIÓN Y PRESUPUESTO INVERMET V°B° J.V.B.

AREA DE INFORMATICA INVERMET V°B° L.A.R.C.

GLOSARIO DE TERMINOS

En el contexto de la presente Directiva, los conceptos utilizados se definen:

Antivirus: Software diseñado para detectar y eliminar virus.

Backup: Copia de seguridad de la información en un dispositivo de almacenamiento, con el fin de poder recuperar la información en caso de daño, borrado accidental o un accidente imprevisto.

Base de Datos: Conjunto de datos que permanecen al mismo contexto almacenados sistemáticamente, los datos pueden aparecer en forma de texto, números, gráficos, sonidos o videos.

Restauración: Volver a poner algo en el estado inicial, una base de datos se restaura en otro dispositivo después de un desastre.

Tape: Cinta magnética que se utiliza para guardar los Backup.

OB: Operador de Backup.

Malware: (del inglés malicious software), también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

Backdoor o puerta trasera: Método para eludir los procedimientos habituales de autenticación al conectarse a una computadora.

Troyano: Término usado para designar a un malware que permite la administración remota de una computadora, de forma oculta y sin el consentimiento de su propietario, por parte de un usuario no autorizado.

Spyware: Programa creado para recopilar información sobre las actividades realizadas por un usuario y distribuirla a agencias de publicidad u otras organizaciones interesadas.

Adware: Programas que muestran publicidad al usuario de forma intrusiva en forma de ventanas emergentes (pop-up) o de cualquier forma.

Spam: Correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptos.

Virus Informático: Es un programa o un segmento de código creado con el objetivo de causar daños en los computadores, el cual puede ocasionar graves consecuencias para el computador que lo almacena.

SDat = Archivo de actualizaciones de formas de virus.

Cortafuegos (firewall en inglés): Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.