"Año de la Diversificación Productiva y del Fortalecimiento de la Educación"

RESOLUCION DE GERENCIA GENERAL N° 004 -2015-GG/SBLM

Lima, 19 de Enero del 2015.

VISTO:

El Informe N° 086-2014-OI/GG/SBLM, de fecha 26 de diciembre del 2014, emitido por la Jefatura de la Oficina de Informática, mediante el cual solicitan se apruebe el Plan de Contingencia 2014 – 2015 de la Sociedad de Beneficencia de Lima Metropolitana – SBLM;

CONSIDERANDO:

Que, mediante el documento del visto, la Jefatura de Informática informa sobre la necesidad de aprobar el Plan de Contingencia 2014 – 2015 de la SBLM;

Que, por Resolución de Contraloría N° 320-2006-CG, publicada el 03 de noviembre del 2006, se aprobaron las Normas de Control Interno, como los lineamientos, criterios, métodos y disposiciones para la aplicación y regulación del control interno en las principales áreas de la actividad administrativa y operativa de las entidades, incluidas las relativas a la gestión financiera, logística, de personal, de obras, de sistemas de información y valores éticos, entre otros. Se dictaron con el propósito de promover una administración adecuada de los recursos públicos en las entidades del Estado;

Que, en el punto 7 del numeral 3.10 de la pre citada Normas de Control Interno se señala que para el adecuado ambiente de control en los Sistemas Informáticos se requiere que estos sean preparados y programados con anticipación para mantener la continuidad del servicio y para ello se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado, donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones en emergencia;

Que, por Resolución de Contraloría N° 458-2008-CG, publicada el 30 de octubre del 2008 se aprueba la "Guía para la Implementación del Sistema de Control Interno de las Entidades del Estado", en cuyo Anexo N° 14 - Glosario de Términos se señala que el Plan de Contingencia es un Instrumento de Gestión que contiene medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la entidad;

Que, es necesario aprobar el Plan de Contingencia 2014-2015, a fin de dar cumplimiento a las normas vigentes sobre la materia;

Que, el Artículo 17.1° de la Ley N° 27444 – Ley del Procedimiento Administrativo General, establece que la autoridad podrá disponer en el mismo acto administrativo que tenga eficacia anticipada a su emisión;

Que, contando con la visación de la Oficina de Informática, y;

..//

RESOLUCIÓN DE GERENCIA GENERAL Nº 004 -2015-GG/SBLM.....2.

De conformidad con las facultades contempladas en el Reglamento de Organización y Funciones, formalizada su vigencia mediante Resolución de Presidencia N° 38-2014-P/SBLM de fecha 29 de Agosto de 2014, y;

SE RESUELVE:

Artículo 1°.- Aprobar, con eficacia anticipada al 01 de Enero del 2014, el Plan de Contingencia 2014-2015 de la Sociedad de Beneficencia de Lima Metropolitana, el mismo que como Anexo, forma parte de la presente Resolución.

Artículo 2°.- Encargar a la Oficina de Informática que realice las acciones que correspondan para la aplicación del presente Plan de Contingencia en la Sociedad de Beneficencia de Lima Metropolitana.

Artículo 3°.- Poner en conocimiento de todo el personal el Plan de Contingencia aprobado en el Artículo precedente.

Regístrese, comuníquese , cúmplase y archívese.

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

Sociedad de Beneficencia de Lima Metropolitana

Arq. JOSÉ RODRÍGUEZ CÁRDENAS
Gerente General

Municipalidad Metropolitana de Lima

SOCIEDAD DE BENEFICENCIA
DE LIMA METROPOLITANA

PLAN DE CONTINGENCIA

INDICE

Local Central
Jr. Carabaya N° 641,
Centro Histórico de Lima
Teléfono
427-6621
www.sblm.gob.pe

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

Local Central
Jr. Cailloma 641,
Cercado, Histórico de
Lima
[illegible]
[illegible]
[illegible]

1 INTRODUCCION

El presente Plan de Contingencia para los años 2014-2015, busca establecer los procedimientos a utilizarse frente a los riesgos a los que están expuestos los componentes de Tecnologías de información que utiliza la Sede de la Sociedad de Beneficencia de Lima Metropolitana, de tal forma que se garantice el restablecimiento del correcto funcionamiento de los servicios en el menor tiempo posible, ante cualquier eventualidad.

Este Plan implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de computo y la información contenida en los diversos medios de almacenamiento, por lo que en este se han analizado los riesgos, como reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que s presente la Contingencia. Por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de desastres, el cual tendrá como objetivo, restaurar el Servicio de Computo en forma rápida y con el menor costo y pérdidas posibles.

Es deber de todos los miembros de la institución, de los funcionarios, directivos, y trabajadores en general, comprender la necesidad de garantizar los servicios, considerando las inversiones en medidas de seguridad informativa como una inversión, que contribuyen en la eficacia y eficiencia de la institución.

El presente Plan de Contingencia podrá servir como un repositorio centralizado para la información, tareas y procedimientos que puedan ser necesarios para facilitar la toma de decisiones a la Alta Dirección, así como desarrollar procesos y definir sus tiempos de respuesta ante cualquier falseo o interrupción. Esto es importante si la causa de la interrupción es tal que una pronta restauración de las operaciones no pueda ser realizada empleando solamente procedimientos operacionales de un día normal.

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

2 DEFINICION

Es el documento de gestión para el buen manejo de las Tecnologías de la Información y las Comunicaciones. Dicho documento contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la institución.

El Plan de Contingencias será revisado anualmente; pero presentarse alguna amenaza deberá ser revisado y evaluado.

El Plan de Contingencias incluye tres componentes.

2.1 Respaldo.

Contempla las medidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

2.2 Emergencia.

Contempla las medidas necesarias durante la materialización de una amenaza. Su finalidad.

Es contrarrestar los efectos adversos de la misma.

2.3 Recuperación.

Contempla las medidas necesarias después de materializada y controlada la amenaza.

Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

El Plan de contingencias expresa los siguientes aspectos:

a) Que recursos materiales son necesarios.

b) Quienes están implicados en el cumplimiento del plan, sus responsabilidades concretas y su rol.

c) Acciones a seguir.

3 PROPOSITO

El propósito del Plan es mantener la continua ejecución de los procesos de misión crítica y sistemas de información apoyados en Tecnologías de Información, en el caso extraordinario que un evento pudiera ocasionar que los sistemas fallen en el mismo de su producción.

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

Local Central
Jr. Cusco N° 541,
Centro Histórico de Lima
427 6520
427 6521
www.sblm.gob.pe

4 ALCANCE

Proveer información sobre los sistemas, lugares, medidas, limitaciones técnicos y/o físicas del Plan de Contingencia de la Sociedad de Beneficencia de Lima Metropolitana; brindando especial atención a los Sistemas de información de la SBLM o aquellos que desde esta se brindan.

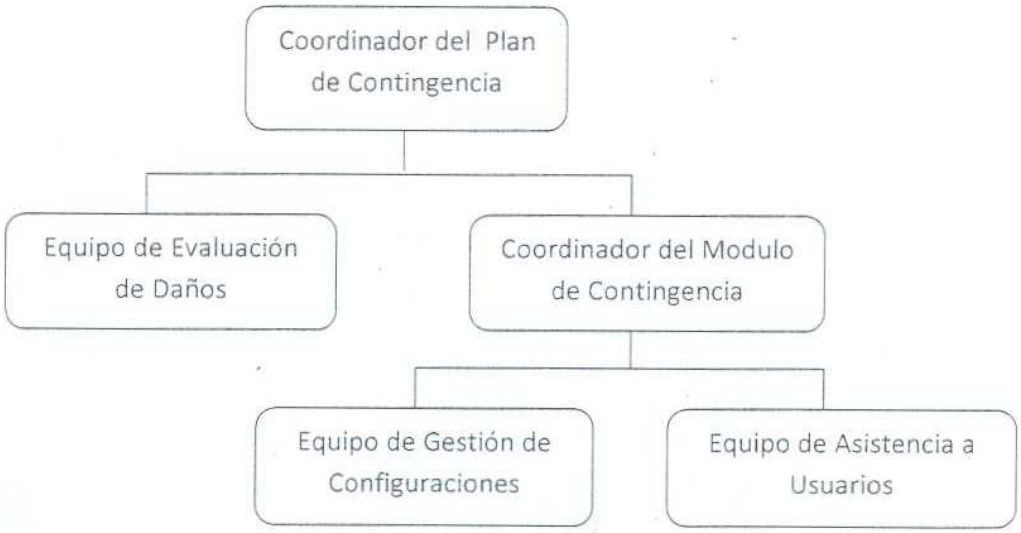
5 OBJETIVOS

a.- Garantizar el normal desarrollo de las actividades diarias de la organización.

b.- Garantizar la integridad, disponibilidad y confidencialidad de la información.

6 ORGANIZACIÓN Y EQUIPOS DE TRABAJO

En el caso de un desastre u otra circunstancia que conlleve la necesidad de operaciones de contingencia, la institución deberá organizarse, para activar la contingencia. Para ello se define la estructura y funciones requeridas por la contingencia, que se activara en conjunto para la restauración en el menor tiempo de las operaciones de la misma.



- El Coordinador del Plan de Contingencia, es el Gerente General, quien determinara que equipos y miembros son responsables de cada función durante las diferentes fases.

- El Coordinador del Modulo de Contingencia, es la Jefe de la Oficina de Informática, y será el responsable de coordinar las operaciones de restauración de los servicios informáticos ante la materialización de una amenaza, definiendo tares y responsabilidades para el Equipo de gestión de Configuraciones y el Equipo de Asistencia a Usuarios.

- El equipo de Evaluación de Daños, se encargara de identificar los efectos provocados por la eventualidad presentada, elaborando un informe teniendo como instrumento de trabajo el Formato Nº 01: "EVALUACION DE DAÑOS" (Ver Anexo).

- El Equipo de Gestión de Configuraciones, es el responsable de restaurar o efectuar las configuraciones en los sistemas afectados por la eventualidad para habilitar los servicios informáticos.

- El Equipo de Asistencia a Usuarios, es el responsable de desarrollar actividades de apoyo y manejo de la emergencia y recuperación de los servicios informáticos con los usuarios de los sistemas afectados por la eventualidad.

7 CRITERIOS PARA RECURRIR AL PLAN

El Plan de Contingencia se activara cuando se paralicen parcial o totalmente las actividades de la Sociedad de Beneficencia de Lima Metropolitana como consecuencia de los fallos en los sistemas de información.

8 UBICACION DE LA INFORMACION CRÍTICA

8.1 Equipos – Servidores

Nº	DESCRIPCION	DETALLE	PROCESADOR	SISTEMA OPERATIVO	DISCO DURO	MEMORIA	ACTIVIDADES
1	SERVIDOR DGAI	SERVIDOR	INTEL XEON 3.40 GHz	MS WINDOWS SERVER 2003	2 DISCOS DE 72 GB SCSI	1 GB DE RAM	SE ALOJAN LAS APLICACIONES Y LAS BASES DE DATOS DE LOS SISTEMAS DE TESORERIA, CONTABILIDAD, LOGISTICA E INMOBILIARIA
2	SERVIDOR SGA	SERVIDOR	INTEL XEON 3.40 GHz	MS WINDOWS SERVER 2003	2 DISCOS DE 72 GB SCSI	1 GB DE RAM	BASE DE DATOS SQL SERVER DE LOS SISTEMAS STD, DBSGI, DBGESINM Y TESORERIA SALDOS
3	SERVIDOR SBLMAPP	PC - Realiza Función de servidor	INTEL PENTIUM III XEON 3.40 GHz	MS WINDOWS SERVER 2003	DISCO DE 140 GB SAS	2 GB DE RAM	SE ALOJAN LAS CONSULTAS Y LOS REPORTES DEL SGA
4	SERVIDOR TEMP	PC - Realiza Función de servidor	INTEL CORE 2 DUO 2.53GHz	MS WINDOWS SERVER 2003	DISCO DE 160 GB SATA	1 GB DE RAM	CONTROLADOR DE DOMINIO
5	SERVIDOR BD-SIGA	PC - Realiza Función de servidor	AMD ATHLOM II x 4	MS WINDOWS SERVER 2003	DISCO DE 500 GB SATA	2 GB DDR3	BASE DE DATOS DEL SGA
6	SERVIDOR PROXY	PC - Realiza Función de servidor	AMD ATHLOM II x 4	LINUX- DEBIAN	DISCO DE 500 GB SATA	2 GB DDR3	PROXY: CONTROL DE ACCESO PARA EL INTERNET
7	SERVIDOR WEB	PC - Realiza Función de servidor	AMD ATHLOM II x 4	LINUX- UBUNTO	DISCO DE 500 GB SATA	2 GB DDR3	REALIZA LA FUNCION DE SERVIDOR WEB, SE ALOJA EL SISTEMA DE PERSONAL Y LA INTRANET
8	SERVIDOR BD-PERSONAL	PC - Realiza Función de servidor	AMD ATHLOM II x 4	MS WINDOWS 7	DISCO DE 500 GB SATA	4 GB DDR3	BASE DE DATOS DEL SISTEMA DE PERSONAL
9	SERVIDOR VPN	PC - Realiza Función de servidor	INTEL CORE 2 DUO 2.53GHz	LINUX- UBUNTO	DISCO DE 500 GB SATA	2 GB DE RAM	SERVIDOR VPN

Local Central
Jr. Carabaya 541,
Centro Histórico de Lima
427-6520
427-6534
www.sblm.gob.pe

Cabe señalare que la actual jefatura de OI, a gestionando el acceso a Internet con línea de 5MB

La Sociedad de Beneficencia de Lima Metropolitana cuenta con el ancho de banda, el cual permite contar con acceso a Internet los 365 días del año, y este servicio lo proporciona la Empresa telefónica S.A.

9 CRITERIOS PARA LA CONTINUIDAD DEL SERVICIO INFORMATICO

9.1 Identificación de activos que pueden ser afectados (Sistemas/aplicaciones/servicios de misión critica)

9.1.1 Nivel Físico

Componente	Detalle
Equipamiento Computacional	Servidores, PCs; Laptops, Impresoras, Escáner; proyector Multimedia y otros periféricos
Equipos de Comunicación	Switch, Router, Modem.
Conectividad LAN	Tendido de Red, Unidades de Distribución de Datos (IDF) ubicados en la SBLM
Conectividad MAN/WAN	Enlaces de Red y Unidades de Distribución de Datos (IDF) a cargo de la SBLM.
Acceso a Internet	Línea convencional para acceso a Internet

9.1.2 Nivel Funcional

Componentes	Detalles
Servicio de Aplicaciones	Software para servicios de aplicaciones web (servicio)
Servicio de Base de Datos	Software gestor de bases de datos
Servicio de Directorio (Dom)	Software de controlador de los usuarios del dominio
Servicio de Archivos	Documentos de Usuarios y Dependencias (en producción)
Aplicaciones Compartidas	Aplicaciones para Windows del PDC
Proxy/Firewall	Servicio para la gestión de los accesos a Internet.

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

9.2 Infraestructura Computacional

9.2.1 Resumen de Computadoras de la SBLM

EQUIPOS DE COMPUTOS			
SEDE CENTRAL		PROGRAMAS	
	TOTAL INSTALADOS		TOTAL INSTALADOS
SISTEMA OPERATIVO (ESTACION DE TRABAJO)		SISTEMA OPERATIVO (ESTACION DE TRABAJO)	
WINDOWS 8 64 BITS	2	WINDOWS 7 64 BITS	8
WINDOWS 7 64 BITS	80	WINDOWS 7 64 BITS	8
WINDOWS 7 32 BITS	17	WINDOWS 7 32 BITS	6
WINDOWS VISTA	0	WINDOWS VISTA	1
WINDOWS XP	112	WINDOWS XP	80
WINDOWS SERVER 2003	6	WINDOWS SERVER 2003	0
WINDOWS 2000	1	WINDOWS 2000	1
UBUNTU	3	UBUNTU	0
CANTIDAD DE EQUIPOS	221	CANTIDAD DE EQUIPOS	96

9.3 Resumen de Impresoras de la SBLM

Tipo de Impresoras	Cantidad
Impresoras Administrables	68
Impresoras en Red	2
Total	70

9.4 Dispositivos de Comunicación de la Red Informática de la SBLM
Sede Jr. Carabaya – Puno

Ubicación/Mar4ca y Modelo	Numero de Puertos
Gerencia de Planeamiento y Presupuesto /3Com	16 puertos
Gerencia de Planeamiento y Presupuesto /Switch Dlink	8 puertos
Unidad de sucesiones /Switch D-LINK DES-1024D	24 puertos
Unidad de sucesiones /Switch TREDNET TE100-S24H/WB	24 puertos
Unidad de Margesí /Switch D-LINK DES-1008d	8 puertos
Unidad Judicial /Switch D-link	8 puertos
Sub Gerencia de Gestión Inmobiliaria- Arrendamiento /Switch SATRA SA-SF1008D	8 Puertos
Sub Gerencia de Gestión Inmobiliaria- Autovaluo /Switch Dlink	16 Puertos
Sub Gerencia de Gestion Inmobiliaria - Recaudación /Switch D-LINK	8 puertos
Gerencia de Negocios Inmobiliarios /Switch Dlink DES-1008D	8 Puertos
Gerencia General /Switch Encore	8 puertos
Gerencia General /Switch D-link	8 puertos
Oficina de Comunicaciones /Switch D-link DES-1008 A	8 puertos
Oficina Sub Gerencia de Logistica/ Switch D-Link	8 Puertos
Unidad de Tramite Documentario / Switch Dlink DES-1008D	8 Puertos
Sub Gerencia de ingenieria y Desarrollo de Proyectos / Switch DLINK	8 Puertos
Sub Gerencia de ingenieria y Desarrollo de Proyectos / Switch 3COM	9 Puertos
Oficina de Control Interistitucional /Switch D-Link	16 Puertos
Servicio Social /Switch	24 Puertos
Sub Gerencia de Logistica /Switch D-Link Des-1024D	24 Puertos
Sub Gerencia de Logistica /Switch	8 Puertos

Sub Gerencia de Contabilidad / Switch	8 Puertos
Sub gerencia de Tesoreria /Switch	8 Puertos
Sub Gerencia de Contabilidad / Switch D-Link Des-1024D	24 Puertos
Gerencia de Planeamiento y Presupuesto /Switch Encore	8 Puertos
Sub Gerencia de logistica- Programacion /Switch Encore	8 Puertos
Informatica/Switch 3COM Model 4228 G – Super Stack3	24 Puertos
Informatica /Switch 3COM Vaseline 2824	24 Puertos
Informatica/Switch DES – 1016D	24 Puertos
SubGerencia de Gestion Inmobiliario	8 Puertos
Informatica /Switch	24 Puertos
TOTAL 31	

9.5 Situación General de los Sistemas

La infraestructura mencionada en el apartado anterior (nivel físico) soporta al nivel funcional, en cual destacaremos las aplicaciones que se han desarrollado a la necesidad requerida en su momento para la administración pública de la Sociedad de >Beneficencia de Lima Metropolitana.

9.5.1 .Aplicaciones de Escritorio Windows

Sistema o Aplicación	Sistema de Gestión de Inmobiliaria (SGI Versión 1.1)
Descripción	Conjunto de módulos que permiten el ingreso de información logística. Estos son: • Módulo de Recaudación • Módulo de Mantenimientos • Módulo de Administración • Modulo de Arrendamiento • Módulo de Gerencia
Base de Datos	La Base de Datos están manejados por el motor SQL Server 2008 y se encuentran en el servidor de base de datos OIE01
Procedencia	Ha sido elaborado por la Oficina de Informática (OI) de la Sociedad de Beneficencia de Lima Metropolitana (SBLM).
Lenguaje de Programación	Se utiliza Java EE 6.0
Código Fuente	Se cuenta con el código fuente.
Manual de Usuario	Si se cuenta con el manual de usuario.
Manual del Sistema	Si se cuenta con la documentación del sistema.
Estado	Se encuentra en uso por parte de los usuarios

Observaciones	

Sistema o Aplicación	Sistema de Trámite Documentario (STD)
Descripción	Permite registrar los Documentos generados con todos sus envíos, registrar el flujo de los documentos y efectuar el seguimiento documentario.
Base de Datos	Se trata de dos archivos: uno con extensión MDF, el cual contiene el conjunto de tablas y otro con extensión LDF, el cual contiene el registro de transacciones. Estos archivos son manejados por el motor SQL Server 2000 y se encuentran en el servidor de base de datos SBLMSIGA.
Procedencia	Ha sido elaborado por la Oficina de Informática (OI) de la Sociedad de Beneficencia de Lima Metropolitana (SBLM).
Lenguaje de Programación	MS Visual Basic 6.0 (versión de producción) / MS Visual Basic 2005 (versión de prueba)
Código Fuente	Se cuenta con el código fuente.
Manual de Usuario	Se cuenta con el manual de usuario.
Manual del Sistema	Se cuenta con la documentación del sistema.
Estado	Se encuentra en uso por parte de la Unidad de Trámite Documentario (UTD), la Gerencia General y de la Oficina de Informática (OI). En el resto de Órganos y Unidades Orgánicas se encuentra en fase de Despliegue (Instalación y Capacitación).
Observaciones	• Anteriormente, el proceso de Trámite Documentario en la Institución se realizaba de forma manual o de forma automatizada con el uso de diferentes aplicaciones en los Órganos y Unidades Orgánicas, lo cual afectaba el rápido seguimiento de los documentos. • Actualmente, el sistema: o Facilita la administración de los documentos y su ubicación. o Permite el control del flujo documentario (recepción y envío). o Genera la hoja de ruta. o Permite imprimir reportes según las condiciones de búsqueda o de filtrado.

Sistema o Aplicación	Sistema Integrado de Administración Financiera - SIAF
Descripción	Permite administrar, mejorar y supervisar las operaciones concernientes a la ejecución de Ingresos y Gasto a través de sus distintas fase para el PIM, Notas Modificatorias, Certificados, Compromiso Anuales, Mensuales, Devengados y Girado; además de permitir la integración de los procesos presupuestarios.
Base de Datos	Su Base de Datos de extensión DCX, el cual contiene el conjunto de tablas relacionadas con extensión DBF.
Procedencia	Ha sido elaborado por el Ministerio de Economía y Finanzas (MEF)
Lenguaje de Programación	MS Visual Fox 8.0 – 9.0 (versión de producción).
Manual de Usuario	Se cuenta con el manual de usuario.
Estado	Se encuentra en uso por parte de las Oficinas Administrativas de la Gerencia de Administración y la Oficina de Presupuesto
Observaciones	• A través de los Módulos del SIAF asignados a la SBLM, se viene registrando la información en línea y de la regularización de datos presupuestales y administrativos de la ejecución de Ingresos y Gastos para el presente periodo 2014. • Oficinas que registran en el SIAF la información en línea: ○ Oficina de Presupuesto: desde el mes agosto viene registrando en el sistema las Notas Modificatorias y los Certificados Presupuestarios. ○ Oficina de Logística: desde el mes de setiembre viene registrando los Compromisos Anuales y Compromiso Mensuales. ○ Oficina de Contabilidad: desde el mes de setiembre viene registrando los registros correspondiente a los Devengados ○ Oficina de Tesorería: desde el mes setiembre viene registrando las operaciones de los Ingresos comprendidas en las fases de los Determinados y Recaudados.

Local Central
Jr. Carabaya 941
Centro Histórico de Lima
427-6820
www.sblm.gob.pe

Sistema o Aplicación	Página WEB
Descripción	• Se desarrolló una pagina web completamente administrable y de acuerdo a lo especificado por la alta dirección con el apoyo de la oficina de comunicaciones.
Base de Datos	La base de datos el mysql 5.1
Procedencia	Ha sido elaborado por la Oficina de Informática (OI) de la Sociedad de Beneficencia de Lima Metropolitana (SBLM).
Lenguaje de Programación	PHP 5.3
Gestor de Contenidos (CMS)	Joomla 2.52
Código Fuente	Se cuenta con el código fuente.
Estado	Esta en producción desde el 09/03/2012 y ya se han recibido

Sistema o Aplicación	Sistema de Inventario de Cementerio web
Descripción	Se desarrolló un sistema web, administrable y de acuerdo a lo especificado por la alta dirección con el apoyo de la oficina de comunicaciones, a fin de tener el inventario de los cementerios de la SBLM. Es sistema es administrado por la Oficina de Comunicaciones
Base de Datos	La Base de Datos están manejados por el motor SQL Server 2008 y se encuentran en el servidor de base de datos OIE01
Procedencia	Ha sido elaborado por la Oficina de Informática (OI) de la Sociedad de Beneficencia de Lima Metropolitana (SBLM).
Lenguaje de Programación	Se utiliza Java EE 6.0
Código Fuente	Se cuenta con el código fuente.
Estado	Esta en producción desde el 09/03/2012 y ya se han recibido

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

Sistema o Aplicación	Sistema de Personal (SISPER)
Descripción	Permite el registro de la información del personal, procesar las planillas de Personal nombrado, contratado, CAS, y practicantes entre otros.
Base de Datos	Se trata de un archivo con extensión DB, el cual contiene el conjunto de tablas. Este archivo es manejado por el motor SQL Anywhere 5.0 y se encuentra en un directorio compartido en el servidor de aplicaciones SBLMDGAI
Procedencia	Ha sido elaborado por el Ministerio de Economía y Finanzas (MEF)
Lenguaje de Programación	Power Builder 8.0

Sistema o Aplicación	Sistema de Contabilidad
Descripción	Permite el registro de la información administrativa contable (documentos fuentes emitidos por los diferentes Órganos y Unidades Orgánicas de la Institución).
Base de Datos	Se trata de un conjunto de tablas Libres con extensión DBF, las cuales se encuentran en el mismo directorio del Sistema en el servidor de aplicaciones SBLMDGAI.
Lenguaje de Programación	MS FoxPro 2.6

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

Local Central
Jr. Cotabaya 041,
Centro Histórico de
Lima
[illegible]
[illegible]
www.sblm.gob.pe

Sistema o Aplicación	Sistema de Tesorería
Descripción	Conjunto de módulos que permiten el ingreso de información. Estos son: • Módulo de Caja: permite el ingreso diario de los pagos por diferentes conceptos tales como venta de formularios, mandas forzosas, ingreso por ventas de menús de los comedores, pensión de Sevilla, pago de matrículas. • Módulo de Fonavi: permite el ingreso las cancelaciones mensuales del Conjunto Habitacional Orbegoso. • Módulo de Control de API, Cementerios y Canevaro: se trata de un conjunto de tres sub-módulos, los cuales permiten la impresión de los recibos de ingreso, registro de ventas, listados contables y listados presupuestales.
Base de Datos	Se trata de un conjunto de tablas Libres con extensión DBF, las cuales se encuentran en el mismo directorio de cada uno de los módulos a los que pertenecen en el servidor de aplicaciones SBLMDGAI.
Lenguaje de Programación	MS FoxPro 2.6
Sistema o Aplicación	Software de Inventario Mobiliario Institucional (SIMI).
Descripción	Permite el registro de la información de los bienes muebles para su remisión a la Superintendencia de Bienes Nacionales (SBN).
Base de Datos	Se trata de un conjunto de tablas Libres con extensión DBF, las cuales se encuentran en el mismo directorio del Sistema en el servidor de aplicaciones SBLMDGAI.
Procedencia	Ha sido elaborado por la Superintendencia de Bienes Nacionales (SBN).
Lenguaje de Programación	MS Visual FoxPro 6.0

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

Local Central
Jr. Carabaya 641
Centro Histórico de Lima

Sistema o Aplicación	Sistema APIMONS (presenta obsolencia)
Descripción	Permite el ingreso de los movimientos diarios por concepto de alquileres. Específicamente: • Mantiene el registro de las Upas • Mantiene el registro de los Comprobantes de pago emitidos manualmente
Base de Datos	Se trata de un conjunto de tablas Libres con extensión DBF, las cuales se encuentran en el mismo directorio del Sistema en el servidor de aplicaciones SBLMDGAI.
Lenguaje de Programación	MS FoxPro 2.6

Sistema o Aplicación	Sistema de Gestión de Abastecimiento (SGA)
Descripción	Conjunto de módulos que permiten el ingreso de información logística. Estos son: • Módulo de Programación: genera el cuadro de Necesidades, realiza la distribución de Bienes y servicios a cada unidad ejecutora vinculando cada clasificador de gasto con las unidades ejecutoras. • Módulo de Adquisiciones: genera la las Órdenes de Compra y Servicio. Prevé, en forma racional y sistemática, la satisfacción de las necesidades de bienes y servicios para el cumplimiento de las metas asignadas.
Base de Datos	Se trata de dos archivos: uno con extensión MDF, el cual contiene el conjunto de tablas y otro con extensión LDF, el cual contiene el registro de transacciones. Estos archivos son manejados por el motor SQL Server 2000 y se encuentran en el servidor de base de datos SBLMSIGA.
Lenguaje de Programación	MS Visual Basic 2005

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

Sistema o Aplicación	Sistema de Información y Alerta Temprana Anticorrupción
Descripción	• Se desarrolló un sistema web inmerso en el portal de la SBLM, cuya finalidad es articular las acciones de la institución, con participación de los trabajadores, usuarios y ciudadanos en general para la priorización de la ética en el desempeño de la función pública y la prevención de lucha contra la corrupción administrable. • El sistema web, recoge mediante interfaces (fichas electrónicas) las denuncias anónimas o públicas.
Base de Datos	La base de datos esta manejado por el motor de SQL server 2008
Procedencia	Ha sido elaborado por la Oficina de Informática (OI) de la Sociedad de Beneficencia de Lima Metropolitana (SBLM).
Lenguaje de Programación	Java EE 6.0
Código Fuente	Se cuenta con el código fuente.
Directiva	Directiva Nº 01-2013-P/SBLM Directiva Nº 02-2013-P/SBLM
Estado	Se encuentra en uso, al servicio de los trabajadores y público en general.
Observación	El sistema se encuentra alojado en el Portal de la SBLM.

9.5.2 Software Commercial

A. Windows 7
B. AutoCAD
C. Microft Project
D. Sistema 10- Presupuesto
E. Windows Server

La Sociedad de Beneficencia de Lima Metropolitana por medio de la actual administración de la OI viene gestionando a realizarse las actividades en el corto y/o mediano plazo para la adquisición de software licenciado, de acuerdo a las necesidades del personal que labora en las oficinas de la entidad en cuanto a los servicios informáticos los cuales determinan el correcto medio de adquisición e utilización de los mencionados software.

9.5.3 Software Libre – Open Source

A. DEBIAN 6.03

9.5.4 Sistemas Informáticos proporcionados por terceros

Nombre del sistema	Entidad proveedoras del sistema
SISPER	Ministerio de Economía y Finanzas
SIAF	Ministerio de Economía y Finanzas
SIMI	Superintendencia Nacional de Bienes Estatales
SISBEN	Programa Integral Nacional para el Bienestar Familiar - INABIF
PDT	Superintendencia Nacional de Administración Tributaria
SAGU	Contraloría General de la República

10 IDENTIFICACION Y EVALUACION DE AMENAZAS

La siguiente tabla muestra las amenazas más comunes que podrían impactar la continuidad y componentes de sistemas y su administración.

	Probabilidad de Amenaza		
Ocurrencia	Alta	Media	Baja
1. Daño a la integridad Personal		X	
2. Perdida de comunicación	X		
3.Destruccion de información		X	
4.Falla de aire acondicionado		X	
5.Corte eléctrico Interrupción		X	
6.Fuego		X	
7.Inundacion/Daño por agua			X
8.Terremotos			X
9.Amenazas de bomba			X
10.Sabotaje/Terrorismo			X
11.Vandalismo			X

11 ACCIONES DE RESPALDO

11.1 Generales

A. Contar con un directorio de los responsables de los servicios obtenidos de terceros tales como el suministro eléctrico, servicio de telefonía, servicio de Internet y servicios de mantenimiento.
B. Contar con un procedimiento para reportar el incidente a las áreas involucradas (Proveedores de Servicios, proveedores de Mantenimiento, etc.)
C. Contar con procedimiento para notificar a los usuarios afectados por la probable baja de los Servicios de comunicación.
D. Contar con procedimiento de ejecución de respaldos de emergencia a la información de los servidores de la Red Informática de la SBLM.

E. Colocar letreros o anuncios que impidan el acceso al personal no autorizado al Área de los Servidores y Unidades de Distribución de datos y que el personal autorizado cuente con Identificación.

11.2 Documentos necesarios previos a las contingencias.

A. Contar con una copia del inventario del equipamiento existente.
B. Contar con un listado de configuraciones de los equipos de cómputo y telecomunicaciones que reside en el Área de Servidores.
C. Contar con documentación al día de contratos de mantenimiento de infraestructura.

11.3 Medios y Materiales.

A. Contar con una copia de cada paquete de software descrito en el Plano Funcional.
B. Programar las tareas de respaldo de la información de los servidores de la Red Informática de la SBLM en periodos que aseguren al máximo el estado de actualización de la misma, ante la eventualidad.
C. Contar con un set de herramientas (maletín o caja) que permitan los trabajos de cambio o Instalación de componentes en los equipos del área de Servidores.

11.4 Acciones preventivas a la contingencia respecto a cada ocurrencia.

11.4.1 Daño a la integridad del Personal

A. Programar al menos 1 simulacro al año.
B. Conocer el manejo de los extintores
C. Contar con botiquines de primeros auxiliaos en áreas estratégicas de la SBLM.
D. Contar con capacitación de primeros auxilios.
E. Implementar alarmas de emergencia en lugares estratégicos de la SBLM.
F. Establecer puntos de reunión dentro y fuera de la SBLM
G. Difundir las rutas de evacuación, así como los sitios de localización de alarmas, extintores.

H. Establecer procedimientos de evacuación.
I. Capacitación permanente y actualizada a los comités de Seguridad en Cómputo.
J. Contar con un directorio del personal y de familiares del personal que labora en el área

11.4.2 Perdida de comunicación.

A. Contar con los planos de Red (Físico y Lógico)
B. Establecer medios y servicios alternativos ante la pérdida de comunicación interna y externa; esto es, contar con equipos para la rápida habilitación de unidades de distribución de datos alternativas y adquirir un servicio de acceso de Internet con una empresa diferente a la que provee el mencionado servicio en condiciones normales.

11.4.3 Destrucción de información

A. El lugar físico donde se encuentran resguardos los expedientes sea un lugar aislado y seguro.
B. Verificar el estado de los equipos de restauración de la información.
C. Contar con medios de respaldo de información.
D. Contar con una bitácora de respaldados de información de los Servidores de la Red Informática de la SBLM.
E. Evitar el acceso a personal no autorizado al Área de servidores.

11.4.4 Falla del aire acondicionado

A. Efectuar el mantenimiento de los equipos de aire acondicionado con una frecuencia de 3 meses.

11.4.5 Corte eléctrico/ Interrupción

A. Contar con el mapa eléctrico del Área de Servidores, identificando los contactos respaldados y regulados.
B. Contar con tierras físicas independientes en el Área de Servidores y Unidades de Distribución de Datos.
C. Contar con una planta de emergencia que suministre energía regulada en el Área de Servidores y Unidades de Distribución de Datos.
D. Supervisar semanalmente el nivel óptimo de combustible, agua, batería, etc.
E. Contar con un plan de mantenimiento semestral con supervisiones mensuales.
F. Contar con mecanismos (dispositivos, tablero de control) de intercambio de alimentación de energía automática ante la caída de línea de del servicio público de energía.
G. Contar con un procedimiento de operación y uno en caso d un mal funcionamiento ante la falla de los Controles automáticos para el intercambio de energía.
H. Contar con un UPS con capacidades necesarias (40% superiores) en el Área de Servidores y Unidades de Distribución de Datos.
I. Determinar semestralmente el tiempo efectivo y real de respaldo de UPS con respecto a las diferentes Cargas.

11.4.6 Fuego

A. El área de logística deberá contar con diagramas de instalaciones eléctricas.
B. Contar con extinguidores cargados.
C. Contar con señalizamientos de rutas de evacuación.
D. Contar con lámparas emergentes con batería.
E. Contar con sistemas de alarmas de humo y fuego.
F. Contar con respaldos internos y externos.

11.4.7 Inundación / Daño agua

A. Colocar en lugares el hardware, software y documentos importantes, evitando las zonas propensas a la inundación ya sea fenómenos naturales o por problemas en los ductos de agua y alcantarillado.

11.4.8 Terremotos, Amenazas de bomba, Sabotaje/Terrorismo, Vandalismo.

A. Contar con sistemas de emergencia, servidor redundante (en una

11.4.9 Deterioro de Equipos (hardware)

A. La SBLM cuenta con un equipo de aire acondicionado, que por su antigüedad su potencia de enfriamiento ha bajado enormemente y debe ser remplazado para mayor seguridad instalándolo en el ambiente donde se ubican los nueve (09) servidores principales de la Sede Institucional.

B. Cada equipo de trabajo se mantiene encendido de 08 a 14 horas interrumpidas de lunes a viernes, en ambiente de trabajo con temperaturas variadas, es por esta razón que los equipos cuando no sean usados deberán de estar apagados para evitar recalentamiento.
C. Se ha debe realizar un mantenimiento semestral preventivo de acuerdo a la necesidad de cada área, y además se realiza el mantenimiento correctivo principalmente en las estaciones de trabajo cuando es necesario.
D. La Oficina de Informática debe contar con un stock mínimo de repuestos que sirven para poder realizar los procedimientos del mantenimiento preventivo de los equipos de la SBLM.
E. Todos los equipos deben de tener mínimamente un supresor de pico o un estabilizador de corriente eléctrica y en el mejor de los casos UPS.
F. Se debe de incluir en el plan de capacitación anual para la SBLM, cursos básicos de buenas prácticas para uso de la PC asignada a su cargo.

11.4.10 Robo Común (Hardware)

A. La SBLM cuenta con puertas de acceso peatonal entre la sede Jr. Carabaya y Puno, en cada puerta ha sido ubicado el personal de vigilancia, los cuales tienen la consigna de no dejar salir ningún equipo sin la previa autorización de control patrimonial.
B. En el caso de equipos pequeños como CD, discos duros, mouse están a cargo de las personas a las cuales se les ha asignado la PC, razón por la cual deben de prever darles la seguridad y custodia del caso.
C. Toda visita de personal ajeno a la OI será anunciada por la secretaria (HeldDesK) y se trata en lo posible de que sea lo más breve posible.

11.4.11 Vandalismo (Hardware)

A. El problema de la seguridad del computador debe ser tratado como un problema importante de dirección, el peligro más temido por los Centros de Información, es el sabotaje. Instituciones que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros.
B. Se debe mantener una estrecha colaboración entre los agentes de vigilancia y los servicios de policía con el fin de evitar actos vandálicos.
C. El personal de Soporte Técnico estará disponible para proteger y mantener operativos los Equipos de las dependencias.
D. Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.
E. El personal de la SBLM debe tener conciencia que se deben de cuidar los equipos informáticos asignados a ellos.

11.4.12 Fallas de Equipos (Software)

A. Diariamente se debe realizar una copia completa de los sistemas de la información institucional contenida en el servidor.
B. Es obligación de los usuarios realizar periódicamente copias de seguridad de sus archivos de trabajo relevantes como medida de seguridad

11.4.13 Equivocaciones (Software).

A. La OI deberá preparar manuales de usuario del uso de los sistemas informáticos implementados en la SBLM.

B. La OI deberá capacitar a los usuarios en el uso de los sistemas informáticos desarrollados por la SBLM.
C. Las copias de respaldo del Sistema Informático le deberá realizar obligatoriamente el Administrador del Sistema al terminar la jornada laboral.

11.4.14 Accesos Internos No Autorizados (Software)

A. Dar a los usuarios el acceso a Red por periodos de tiempo o permanente según el caso.
B. Verificar y monitorear la red.
C. Está prohibido el compartir usuarios y claves, siendo responsabilidad del usuario a quien fue asignado.
D. El Jefe de cada dependencia deberá presentar un documento por escrito, indicando los usuarios que podrán acceder a compartir recursos en la Red Institucional.
E. El responsable de cada dependencia deberá presentar un documento por escrito indicando los usuarios que podrán tener una cuenta de correo.
F. El responsable de cada dependencia deberá presentar un documento por escrito, indicando los usuarios que laboraran en el fin de semana, días feriados, etc.

11.4.15 Robo De Datos (Software)

A. Las copias de los sistemas están bajo custodia del Administrador de Red, y queda terminantemente prohibido llevar información fuera de la Institución por cualquier medio.
B. Las copias de la información de las PC's es responsabilidad del usuario asignado y queda terminantemente prohibido llevar esta información fuera de la Institución por cualquier medio.

11.4.16 Fraude Informático (Software)

A. Se debe de evitar la deficiencia en la administración de la operación. Falta de control de documentos y de procedimientos de autorización, regulando cambios del sistema y alteraciones a los ficheros de datos.
B. Está prohibido alterar, dañar o destruir los sistemas, redes o programas.
C. Implementar registros de auditoría en los sistemas

11.4.17 Virus Informático (Software)

A. La SBLM ha adquirido un antivirus llamado Avira Antivir Profesional, instalado en un Servidor dedicado para su actualización en todas las PC's.
B. La empresa Avira Antivir Professional actualiza diariamente su Base de Datos y envía una actualización a todos sus clientes, pues es la única manera de contrarrestar la amenaza de agentes externos que provoquen fallos en el Hardware y/o Software de los equipos de la Red.
C. El antivirus Avira detecta si el email contiene un archivo ejecutable y lo elimina.
D. El usuario debe de hacer copias de seguridad. Mantenga copias de respaldo en buen estado para sus datos y programas más importantes. Esto no solo lo protegerá de los virus, sino también de un serio fallo del hardware.
E. No utilice USB, si es portador de virus.
F. La OI deberá de implementar mecanismos de recuperación de archivos de los discos duros.
G. La descarga de software libre debe de ser realizada desde el web del autor.
H. Tener en cuenta cualquiera de estos eventos puede ser sospechoso de infección por virus.

- ¿Está tomando más tiempo del habitual para cargar programas, o le parece que en general la maquina esta "lenta"?
- ¿Aparecen mensajes de error no habituales?
- ¿Parece haber disminuido el tamaño de la memoria?
- ¿Se mantienen encendidas las luces del usb como solía parpadear antes?
- ¿Desaparecen ficheros sin motivos?

I. Si su computadora está infectada, comunique de inmediato a la OIE-Soporte Técnico.

11.4.18 Accesos Externos No Autorizados (Software)

A. Se debe configurar el Firewall en nivel avanzado.
B. Se debe tener actualizado la relación de usuarios registrados en la Red Institucional.
C. Se debe tener actualizado la relación de usuarios en cada Sistema Informático.
D. Se debe tener actualizado la relación de usuarios cuentas de correo interno
E. Escanear puertos para verificar que no quede posibilidad de alguna vulnerabilidad del Servidor proxy y Firewall.
F. La información se debe clasificar en: secreta, confidencial, privada y pública.

12 ACCIONES DE EMERGENCIA

12.1 Generales.

Activar las operaciones de contingencia, debiendo iniciarse de manera inmediata la identificación de los efectos provocados por la eventualidad presentada, elaborando un informe conforme a lo detallado en el Formato Nº 01: "EVALUACION DE DAÑOS", lo cual estará a cargo de del Equipo de Evaluación de Daños.

12.2 Acciones durante la Contingencia respecto a cada ocurrencia.

12.2.1 Daño a la integridad del Personal Accionar las alarmas de emergencia.

A. Utilizar las botas e impermeables para poder salir o ingresar al Área de Servidores (OI) En caso de inundación.
B. Dirigir a los usuarios en la evacuación e información de salidas de emergencia.
C. Priorizar la evacuación.
D. Llamar al (Numero de emergencias) o Centro de emergencia de Lima Metropolitana.

12.2.2 Perdida de comunicación

A. Establecer unidades de distribución de datos alternativas en el caso de la perdida de comunicación interna.
B. Configurar al acceso de Internet mediante el servicio adquirido con una empresa diferente a la que provee el mencionado servicio en condiciones normales.

12.2.3 Destrucción de Información

A. Restablecer la información, tomando como referencia la bitácora de respaldados de información de los Servidores de la Red Informática de la SBLM.

12.2.4 Falla del aire acondicionado

A. Abrir ventanas para mantener la ventilación en el área de servidores.
B. Apagar los equipos de cómputo menos prioritarios a fin de disminuir el calor del ambiente.

- ¿Está tomando más tiempo del habitual para cargar programas, o le parece que en general la maquina esta "lenta"?
- ¿Aparecen mensajes de error no habituales?
- ¿Parece haber disminuido el tamaño de la memoria?
- ¿Se mantienen encendidas las luces del usb como solía parpadear antes?
- ¿Desaparecen ficheros sin motivos?

I. Si su computadora está infectada, comunique de inmediato a la OIE-Soporte Técnico.

11.4.18 Accesos Externos No Autorizados (Software)

A. Se debe configurar el Firewall en nivel avanzado.
B. Se debe tener actualizado la relación de usuarios registrados en la Red Institucional.
C. Se debe tener actualizado la relación de usuarios en cada Sistema Informático.
D. Se debe tener actualizado la relación de usuarios cuentas de correo interno
E. Escanear puertos para verificar que no quede posibilidad de alguna vulnerabilidad del Servidor proxy y Firewall.
F. La información se debe clasificar en: secreta, confidencial, privada y pública.

12 ACCIONES DE EMERGENCIA

12.1 Generales.

Activar las operaciones de contingencia, debiendo iniciarse de manera inmediata la identificación de los efectos provocados por la eventualidad presentada, elaborando un informe conforme a lo detallado en el Formato Nº 01: "EVALUACION DE DAÑOS", lo cual estará a cargo de del Equipo de Evaluación de Daños.

12.2 Acciones durante la Contingencia respecto a cada ocurrencia.

12.2.1 Daño a la integridad del Personal Accionar las alarmas de emergencia.

A. Utilizar las botas e impermeables para poder salir o ingresar al Área de Servidores (OI) En caso de inundación.
B. Dirigir a los usuarios en la evacuación e información de salidas de emergencia.
C. Priorizar la evacuación.
D. Llamar al (Numero de emergencias) o Centro de emergencia de Lima Metropolitana.

12.2.2 Perdida de comunicación

A. Establecer unidades de distribución de datos alternativas en el caso de la perdida de comunicación interna.
B. Configurar al acceso de Internet mediante el servicio adquirido con una empresa diferente a la que provee el mencionado servicio en condiciones normales.

12.2.3 Destrucción de Información

A. Restablecer la información, tomando como referencia la bitácora de respaldados de información de los Servidores de la Red Informática de la SBLM.

12.2.4 Falla del aire acondicionado

A. Abrir ventanas para mantener la ventilación en el área de servidores.
B. Apagar los equipos de cómputo menos prioritarios a fin de disminuir el calor del ambiente.

12.2.5 Corte eléctrico/Interrupción

En caso de interrupción del suministro eléctrico en lapsos cortos consecutivos.

A. Comunicar de inmediato al Área de Servicios Generales – Sub Gerencia de Logística
B. Monitorear el UPS cada 20 min. para programar acciones mayores.

En caso de una interrupción del suministro eléctrico no mayor a una hora.

A. Comunicarse con el área de servicios generales de la Sub Gerencia de Logística para la supervisión de la Planta de emergencia.
B. Monitores el UPS cada 10 min, para programar acciones mayores.
C. Apagar los equipos informáticos, hasta que se restablezca el servicio.

En caso de una interrupción del suministro eléctrico mayor a una hora

A. Desconectar los equipos informáticos.
B. Comunicar a la Sub Gerencia de Logística a fin de que restablezca el servicio.

12.2.6 Fuego

A. Utilizar los extinguidores por personal capacitado.
B. Respetar los señalamientos de rutas de evacuación.
C. Si es necesario, utilizar lámparas emergentes con batería.
D. Activar el sistema de alarmas.
E. Asegurar que se tengan los respaldos externos.
F. Apagar y desconectar los equipos de cómputo.

12.2.7 Inundación/Daño por agua

A. Activar y desconectar equipos de cómputo
B. Contar con bolsas de plástico para cubrir servidores y documentos importantes que puedan mojarse.

12.2.8 terremotos, Amenazas de bomba, Sabotaje/Terrorismo, Vandalismo

A. Activar los sistemas de emergencia tales como alarmas de emergencia, extintores, sistemas de alarmas de detección de humo y fuego, servicios de respaldo

12.2.9 Deterioro de Equipos

A. Realizar el diagnostico correspondiente al equipo afectado.
B. Llenar la Hoja de Servicio de Atención al Usuario: Fecha, hora, trabajador, dispositivos dañados, motivo, detalle del motivo, usuario. Dicha ficha estará en formato impreso, siendo responsabilidad del técnico de la OI; el llenado correspondiente de acuerdo a diagnostico realizado. De ser necesario elaborar informe técnico para la baja. La OI comunicara al Encargado inmediato adjuntando el informe técnico correspondiente.
C. No cambiar la ubicación del mobiliario y equipo asignado a cada dependencia, sin comunicar a la OI.

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

12.2.10 Fallas de Equipos

A. Realizar el diagnostico correspondiente al equipo afectado.
B. El usuario o el responsable que note cambios en su equipo se comunicara al anexo 284 a fin de que se le asigne un soporte que revise su equipo.

A. El operador de soporte deberá llenar la ficha técnica de atención fecha, hora, trabajador, dispositivos dañados, motivo, detalle del motivo, detalle del motivo.

12.2.11 Robo de Datos.

A. Identificar el equipo terminal (PC) desde donde se hurto la información del disco duro o él Servidor Principal.
B. Identificar los posibles usuarios que normalmente acceden a sus recursos desde esa Pc.
C. Emitir un informe de pérdidas de información a fin de sancionar a los responsables del hecho.
D. Recuperar la información a través de los Backups.

12.2.11.1 Fraude Informático

A. Identificar el equipo terminal (PC) desde donde se modifico la Base de datos de un Sistema Informático del Servidor Principal.
B. Identificar los posibles usuarios que accedieron a sus recursos desde esa Pc.
C. Emitir un informe de pérdidas de información a fin de sancionar a los responsables del hecho.

12.2.11.2 Virus Informáticos

A. Identificar los equipos terminales (PC's) desde donde se produjo la infección.
B. identificar el medio de contagio, nombre del virus y su acción.
C. Informar inmediatamente a la OIE a fin de coordinar con el proveedor de antivirus para que actualice su aplicación.

12.2.11.3 Accesos No Autorizados Externos

A. Identificar el IP del equipo terminal externo de desea conectarse al Servidor.
B. Imposibilitar su futuro acceso y comunicar para las acciones legales correspondientes.

13 ACCIONES DE RECUPERACION

13.1 Acciones después de la Contingencia respecto a cada ocurrencia.

13.1.1. Daño a la integridad del Personal.

A. Brindar los primeros auxilios a las personas que lo requieran
B. Realizar un recuento de los daños causados.
C. Realizar un informe con los hallazgos y emitir a la Alta Dirección.
D. Tomar acciones de acuerdo al informe emitido.
E. Retroalimentar los planes de contingencia con lo aprendido en la última contingencia.

13.1.2 Perdida de comunicación

A. Verificar los sistemas de comunicación internos y externos que garanticen la continuidad de las operaciones de la organización.

13.1.3. Destrucción de Información

A. Analizar los medios de acceso y el mecanismo utilizado para la destrucción de la información
B. Establecer mecanismos y procedimiento de seguridad de la información que eviten la destrucción de la información en la forma identificada.

13.1.4. Fala del aire acondicionado

A. Solicitar de inmediato al área de servicios generales el mantenimiento de los equipos del aire acondicionado.

13.1.5. Corte eléctrico/ Interrupción

A. Brindar un tiempo de gracia (depende de la magnitud de la contingencia) para restablecer los equipos activos y servicios.
B. Restablecer los equipos activos y servicios que se dieron de baja, en forma paulatina.
C. Validar el correcto funcionamiento de los equipos activos y servicios.
D. Identificar los posibles daños de los equipos activos.
E. Notificar a los usuarios afectados sobre el restablecimiento de los servicios y su condición.
F. Evaluar los daños de los equipos activos, planta de emergencia, UPS y canalizarlos a las aéreas correspondientes.

13.1.6. Fuego o Inundación/Daño por agua

A. Verificar las copias de seguridad
B. Restaurara las copias de seguridad

13.1.7 Terremotos, Amenazas de bombas, Sabotaje/Terrorismo, Vandalismo

A. Evaluar el daño causado y emitir informe.
B. Verificar las copias de seguridad.
C. Restaurar las copias de seguridad.

13.1.8. Deterioro de Equipos

A. realizar un análisis costo beneficio del número de equipos que se encuentran deteriorados u obsoletos a fin de planificar la compra de su reemplazo.

13.1.9. Robo Común

A. Identificar y cuantificar exactamente el robo
B. La Sub Gerencia de logística emitirá un informe a la Gerencia de Asesoría Legal a fin de proceder con las acciones legales.
C. Sin perjuicio de las acciones legales, se debe de reemplazar lo robado a fin de no afectar el servicio que brinda la SBLM.

13.1.10 Vandalismo

A. Identificar y cuantificar exactamente el robo.
B. Evaluar la posibilidad de pedir refuerzo de personal a los servicios de policía y de otras instituciones.
C. Se elabore un informe del evento ocurrido.

13.1.11 Fallas de Equipos

A. Evaluar los equipos dañados.
B. elaborar informe técnico conteniendo la información de la solución para tener el equipo operativo.

13.1.12 equivocaciones de Equipo

A. Evaluar la razón por la cual el usuario se equivoco al registrar datos.
B. Corregir el error presentado e informar a fin de tomar las acciones correspondientes con las personas que cometieron el error.

13.1.13 Accesos No Autorizados Internos

A. Analizar como el usuario logro acceder a donde no estaba autorizado.
B. Desconexión Automática
C. Elaborar informe de acceso no autorizado.
D. Verificar los servicios de red Proxy y Firewall a fin de corregir el error presentado.

13.1.14 Robo de Datos (Lógico).

A. Cuantificar la información perdida.
B. Si encuentra cuentas fraudulentas o acceso a su PC sin autorización, póngase en contacto con al OI a fin de evaluar el hecho.
C. Si su información personal está siendo usada para actividades fraudulentas, repórtelo a la Gerencia de Asesoría Legal. Lleve consigo una copia del archivo en caso necesite una prueba del crimen para mostrarlo.

13.1.15 Virus Informáticos.

A. Eliminar el virus y verificar la información por parte del usuario.
B. Informar a la empresa proveedora del antivirus.
C. El equipo de Soporte Técnico evaluara en los 3 días posteriores la performance de dicho equipo y determinara su reinstalación de seguir presentando problemas.

14 LISTA DE RECOMENDACIONES

14.1 Aspectos Generales de la Seguridad de Información para ser Aplicadas en la SBLM.

La seguridad de la información no es un mito es una realidad, de ahí que resulte obvio el interés creciente que día a día se evidencia sobre este aspecto de la nueva sociedad informática. Ladrones, manipuladores, saboteadores, espías, etc. Reconocen que la Oficina de Informática de la SBLM es su nervio central, que normalmente tiene información confidencial y que, a menudo, es vulnerable a cualquier ataque.

La seguridad de la información tiene dos aspectos:

i. Consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata se datos personales, y mantenimiento de la seguridad en el caso de datos institucionales.
ii. protección es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

En general, la protección de los datos requiere ejercer un control sobre la lectura, escritura y empleo de esa información. Para obtener mayor eficiencia en la protección se debe tener siempre presente la protección de los datos, el mantenimiento de la privacidad y la seguridad del secreto. El secreto se logra cuando no existe acceso a todos los datos sin autorización.

Los equipos de Producción y Desarrollo de Sistemas deben entender que las medidas de seguridad han llegado a ser criterios de diseño tan importantes como otras posibilidades funcionales. así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

a) **Privacidad**

Cada usuario ingresa un nombre de usuario y una clave particular para acceder a los servicios de la Red.

Al conectarse a la red, el usuario encontrará que tiene asignado, por defecto, una unidad lógica llamada (es lo que se recomienda como propuesta) donde hay una carpeta que debería llevar su nombre de usuario o el de la oficina a la que pertenece; sobre esta carpeta se tiene accesos y permisos para crear, leer escribir y eliminar archivos personales, estos permisos han sido asignados por el Administrador de Red.

Como grupo de trabajo también tiene asignado, por defecto, una unidad lógica llamada (se debe asignar una letra a dicha unidad compartida) donde se encuentra una carpeta con las siglas correspondientes a la dependencia donde pertenece, dentro de esta carpeta, encontrara sub carpetas con las siglas de las divisiones, oficinas según corresponda, este usuario únicamente sobre esta sub carpeta tiene accesos y permisos para crear, leer, escribir compartir y eliminar archivos institucionales de la SBLM.

La privacidad adecuada puede lograrse cuando los datos que puedan obtenerse no pueden enlazarse a individuos específicos o no pueden utilizarse para imputar hechos.

b) **Seguridad**

Al conectarse a la Red, el usuario encontrara que tiene asignado, por defecto, una unidad lógica llamada donde se encuentran todos los Sistemas informáticos de la Sede; el usuario solo tendrá acceso a las capetas de los Sistemas que se le han asignado para realizar sus funciones.

En esa carpeta de sistema, el usuario puede leer y modificar los archivos a través de su aplicativo correspondiente.

Dentro de cada Sistema Informático se solicita que cada usuario ingrese un nombre derecho a algunas opciones dentro del sistema, pues el único que tiene todas las opciones disponibles es el administrador del Sistema.

c) **Integridad**

Los sistemas que se van a desarrollar serán analizados y diseñados en forma global. Cada sistema debe contener procesos que estén intrínsecamente relacionados.
Garantizar la integridad de los datos mediante la implementación escrupulosa de varios conceptos clave, como los que se incluyen a continuación:
Normalizar datos, Explica el proceso que consiste en perfeccionar las definiciones de datos para eliminar grupos repetidos y dependencias innecesarias.
Definir reglas de empresa, Explica la forma en que las reglas de empre controlan la manipulación de los datos de la aplicación y pueden ser reutilizadas por otras aplicaciones.
Proporcionar integridad referencial, Describe la forma en que la integridad referencial evita que se dañen los datos.

Validar los datos, Explica la comprobación de intervalos, la validación de campos y formas mas complejas de validación de datos.

d) **Consistencia**

Los datos que se ingresan a los sistemas son en formularios de registro de tipos carácter, entero, real e imagen en algunos casos.

La información que resulta del procesamiento de datos se muestra en formatos prediseñados por cada Sistema Informático.

e) **Base de Datos**

Cada Sistema Informático cuenta con su respectiva Base de Datos, la cual cumple con las reglas de normalización; la gestión o administración de la base de datos se realiza a través del Sistema.

En el Plan de Sistema de Información de la Sociedad de Beneficencia de Lima Metropolitana se tiene previsto integrar los Sistemas de información para ser manejados por un Gestor de Base de Datos como puede ser MySql o Sql Server.

f) **Veracidad**

Para acceder a la Red, se valida al usuario y su respectiva contraseña, además se controla y supervisa los servicios brindados a cada usuario y la manipulación de los archivos.

Cuando el usuario ingresa a cada Sistema Informático queda almacenado su nombre en un registro, pues contiene un campo cada tabla, que indica quien manipula esa información además de los impresos para llevar el control de la productividad de cada trabajador.

14.2 Control De Acceso a la Oficina de Informática de la SBLM.

La libertad de acceso a esta dependencia puede crear un significativo problema de seguridad. El acceso normal debe ser dado solamente a la gente que regularmente trabaja en esta dependencia.

Cualquier otra persona, de otro modo puede tener acceso únicamente bajo control, mantener la seguridad física de esta dependencia es la primera línea de defensa.

Para ello se ha tomado en consideración el valor de los datos, el costo de protección, el impacto Que la perdida que podría tener en Sociedad de Beneficencia de Lima Metropolitana y la motivación, competencia y oportunidades de la gente que podría querer dañar los datos o el sistema.

Se tendrá que implementar los siguientes tipos de acceso:

Forma Institucional.- El acceso a esta dependencia se identifica en el área de Recepción Institucional solo a personal autorizado, asignándole una identificación.
Forma Interna:- Existen varias aéreas funcionales.

A. **Soporte Técnico.**
El acceso al cuarto de servidores es SOLAMENTE a trabajadores de la Oficina de Informática.

B. **Desarrollo y Programación.**
El acceso a estas aéreas es para los trabajadores en general previo permiso y coordinación con el jefe de Informática.

C. **Acceso Limitado a los terminales.**
Los terminales que no tienen la debida protección pueden ser mal empleados por personal interno o externo para fines no institucionales.

Cualquier terminal que pueda ser utilizado como acceso a los datos de un Sistema controlado, deberá estar ubicada en un área calificada como segura, de tal manera que no sean usados, excepto por aquellos que tengan autorización para ello.

Igualmente, se deberá considerar la mejor manera de identificar a los operadores de terminales del Sistema, y el uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado.

Las restricciones que el Administrador de Red debe aplicar:

- ✓ Determinar los periodos de tiempo de cada usuario en un terminal por periodos semanales en base a reportes.
- ✓ Designación de los permisos y accesos a cada usuario.
- ✓ Designación de terminal por usuario.
- ✓ Limitación del uso de programas licenciados por cada usuario y/o terminal.
- ✓ Determinación del tiempo de validez de las contraseñas.

D. **Control de Acceso a la Información**
Se sabe que algunos usuarios o extraños (personal no autorizado) quieren encontrar formas de acceder al Sistema y consecuentemente a la Base de datos para descubrir información reservada.

Deben existir programas para proteger e impedir la instalación de software ilegal y sin licenciamiento en sus terminales; y a la vez controlar a los usuarios y sus derechos de acceso, ya sea por grupos individualmente.

El uso del programa puede conferir al usuario algunos de los privilegios que corresponden al controlador de dichos programas.

La transferencia de privilegios es adecuada si el programa actúa como filtro de la información.

Palabra de Acceso (Password)
Es una palabra especial o código que debe teclearse al sistema informático antes que realice un proceso crítico y determinante.

Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados.
La clave que el usuario maneje no debe ser trasmitida a otro usuario por ningún medio.

La clave debe ser mayor a 8 caracteres, y de preferencia que contenga números y letras.
No deben considerar los nombres, teléfonos o fechas de nacimiento como claves.

La identificación de un individuo debe ser muy difícil de imitar y copiar.
Aunque su nombre pueda ser único, es fácil que cualquiera que observe; a quienes tienen acceso al sistema; lo copie, por lo que no es una clave adecuada.

Una vez que se obtiene una clave de acceso al sistema. Esta se utiliza para entrar al sistema de la base de datos desde el sistema operativo.

A fin de proteger el proceso de obtención de una clave a un Sistema Informático, el usuario inventa su clave de acceso, la cual consiste de unas cuantas letras y/o números elegidas por él.

Un intruso puede intentar descubrirla de dos maneras:
Observando el ingreso de la clave.

Utilizando el método de ensayo y error para introducir posibles claves de acceso y lograr acceder.

El Sistema Informático debe cerrarse después que un usuario no autorizado falle dos veces al intentar ingresar una clave de acceso.

Las claves de acceso no deben ser largas puesto que son más difíciles de recordar por ser la Sociedad de Beneficencia de Lima Metropolitana una Institución pública, es recomendable que el Administrador de Red asigne y actualice en coordinación con cada usuario y de forma periódica el password a los usuarios.

No se puede depender de que la ausencia de un trabajador responsable de un computador trabe la operatividad normal de una institución, por lo que puede ser necesario el establecimiento de un procedimiento de tener un duplicado de los password asignados, bajo un esquema de niveles jerárquicos, en sobre lacrado, debiendo utilizar un cuaderno de control, cuando exista la necesidad de romper el sobre lacrado (anotando fecha, hora, motivo, etc.), así como un procedimiento de cambio de password periódicos y por dichas eventualidades.

e) **Niveles de Acceso.**
Los Programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados Sistemas Informáticos, con su correspondiente nivel de acceso

Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

Nivel de consulta de la información no restringida o reservada.
Nivel de mantenimiento de la información no restringida o reservada.
Nivel de consulta de la información incluyendo la restringida o reservada.
Nivel de mantenimiento de la información incluyendo la restringida.

✓ Nivel de Consulta de la Información
El privilegio de lectura está disponible para cualquier usuario y solo se requiere un conocimiento de la estructura de los datos, o del Sistema de otro usuario para lograr el acceso. La autorización de lectura permite leer pero no modificar la base de datos.

✓ Nivel de Mantenimiento de la información consiste en:
Ingreso. Permite insertar datos nuevos pero no se modifica el ya existente.
Actualización. Permite modificar la información pero no la eliminación de datos.
Borrado-Permite eliminación
Un usuario puede tener asignados todos, ninguno o una combinación de los tipos de autorización anteriores.

La forma fundamental de autoridad la tiene el administrador del Sistema Informático correspondiente, que entre otras cosas puede crear, modificar y eliminar usuarios además de asignar algunos accesos dentro del sistema.

Esta forma de autorización la realiza un trabajador de la institución que tiene asignados ese sistema a su cargo, es comúnmente llamado "supervisor", y los demás usuarios son llamados "operadores".

F. **Destrucción**

Sin adecuadas medidas de seguridad la Sociedad de Beneficencia de Lima Metropolitana puede estar a merced no solo de la destrucción de la información sino también de la destrucción de todo el Equipo informático.

La destrucción del equipo puede darse por una serie de desastres como son: incendios, inundaciones, sismos, o posibles fallas eléctricas, etc.

Cuando se pierden los datos y no hay disponibles copias de seguridad, se han de volver a crear los archivos.

De hecho, se puede comprobar como una gran parte del espacio en disco está ocupado por archivos, que es útil tener a mano pero que no son importantes para el funcionamiento normal.

Hay que proteger también ante una posible destrucción del hardware o Software por parte de personal no honrado.

G. **Revelación o Infidencia.**

La revelación o infidencia es otra forma que utilizan los malos empleados para su propio beneficio.

La información, que es de carácter confidencial, es vendida a personas ajenas a la institución. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:
Control del uso de información es paquetes abiertos o cintas y otros datos residuales.

La información puede ser o conocida por personas no autorizadas, cuando se deja en paquetes abiertos. O cintas que otras personas pueden usar.

Se deben tomar medidas para deshacerse del almacenaje secundario de información importante o negar el uso de esta a aquellas personas que pueden usar mal los datos residuales de estas. Mantener datos sensitivos fuera del trayecto de la basura.
Preparar procedimientos de control para la distribución de información.

H. Modificaciones

La importancia de los datos que se modifican de forma ilícita, esta condicionada al grado en que la Sociedad de Beneficencia de Lima Metropolitana depende de los datos para su funcionamiento y toma de decisiones.

Si fuera posibles, esto podría disminuir su efecto si los datos procedentes de las computadoras que forman la base de la toma de decisiones, se verificaran antes de decidir.

Hay que estar prevenido frente a la tendencia a asumir que "si viene del Sistema Informático, debe ser correcto."

Adicionalmente a proteger sus programas de aplicaciones como activos, es a menudo necesario establecer controles rígidos sobre las modificaciones a los programas, para estar seguros de que los cambios no causen daños accidentales o intencionados a los datos o a su uso no autorizado.

Deben ser considerados como medidas de seguridad para proteger los datos en el sistema, las limitaciones en el ámbito de los programas de aplicación, auditoria y pruebas, revisiones de modificaciones, exclusión cuando sea necesario de los programas de aplicación.

Particular atención debe ser dada al daño potencial que pueda efectuar un programador a través de una modificación no autorizada.

Nuestra mejor protección contra la perdida de datos consiste en hacer necesario de los programas de aplicación.

Particular atención debe ser dada al daño potencial que pueda efectuar un programador a través de una modificación no autorizada.

Nuestra mejor protección contra la perdida de datos consiste en hacer copias de seguridad, almacenando copias actualizadas de todos los archivos valiosos en un lugar seguro y realizar una bitácora con los respectivos documentos de autorización firmados por la Jefatura de Informática.

Los usuarios deben ser concientizados de la veracidad de formas en que los datos pueden perderse o deteriorarse.

Se debe realizar la respectiva Directiva en la cual contenga reglas y normativas pueden incorporarse en un Programa de Capacitación.

I. **Política y Responsabilidad de la Seguridad**

Es necesario que la Administración de Red en coordinación con el Jefe de Informática, con los responsables de los equipos de desarrollo y programación y soporte de la SBLM defina políticas de seguridad, en las cuales se deben tener en cuenta que:

La seguridad debe ser considerada desde la fase de diseño de un sistema, como parte integral del mismo.

Deberá darse mayor importancia a la toma de medidas de seguridad, teniendo siempre presente que es indispensable y que es prioritario, no solo para el buen funcionamiento sino también para el mantenimiento del sistema.

Las políticas de seguridad deben ser aportadas por la Gerencia General, los cuales deben ser motivados de manera que tengan un rol importante.

Los encargados del equipo de Soporte Técnico, aquellos que son responsables de gestionar la seguridad informática en la organización, han de considerar las siguientes medidas:
Distribuir las reglas de seguridad.
Escribir en una lista las reglas básicas de seguridad que los usuarios han de seguir para mantener la seguridad y ponerlas en un lugar público destacado.

Se debe considerar la posibilidad de que el Equipo de Producción capacite y distribuya las reglas a todos los Usuarios.

Establezca una línea de comunicación sobre seguridad.

El equipo de Desarrollo y Programación también debe de informar sobre violaciones de la seguridad o actividades sospechosas.

14.3 Recomendaciones en Relación al Centro de Sistemas de Información /OI

A. Es recomendable que la Oficina de Informática no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados. (Se debe tener en cuenta que hay una propuesta de traslado al edificio de Jr. Huancavelica de propiedad de la SBLM)

B. Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor (inconvenientes para el equipo de cómputo), puede ser un riesgo para la seguridad, salvo que tenga protectores de ventanas de fierro.

C. El acceso a la Sala de Servidores /OI debe estar restringido al personal no autorizado.

D. El personal de la SBLM deberá tener su carnet de identificación siempre en un lugar visible.

E. Se debe establecer un medio de control de entrada y salida de visitas a la Oficina de Informática.

F. El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.

G. Deben establecerse controles para una efectiva disuasión, a tiempo, de los intentos no autorizados de acceder a los sistemas y a los archivos de información que contiene.

H. Se recomienda establecer políticas para la creación de los password y establecer periodicidad de cambios de los mismos.

I. Establecer políticas de autorizaciones de acceso físico al ambiente y de establecer periodicidad de cambios de los mismos.

J. Establecer política de control de entrada y salida del personal, así como de los paquetes u objetos que portan,

K. Los controles de acceso, el acceso en si y los vigilantes deben estar ubicados de tal manera que son sea fácil el ingreso de una persona extraña.

L. En caso que ingresara algún extraño a la OI, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo, se debe asignar a una sola persona la responsabilidad de la protección de los equipos en cada dependencia.

M. Se debe de administrar la Cintoteca, bajo la lógica de almacén

N. Esto implica ingreso y salida de medios magnéticos (sean cartuchos, Discos removibles , CD"s, ect.) obviamente teniendo más cuidado con las salidas.

O. La cincoteca, que es el almacén de los medios magnéticos (sean cartuchos, Discos removibles, CD"s, etc. Y de la información que contienen, se debe controlar para que siempre haya determinado grado de temperatura y de humedad.

P. Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad y el control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

14.4 Recomendaciones para el mantenimiento de medios de almacenamiento.

Las cintas magnéticas y cartuchos deben guardarse bajo ciertas condiciones, con la finalidad de garantizar una adecuada conservación de la información almacenada:

a) **Cinta Magnéticas:**

Las recomendaciones pare el buen mantenimiento de las cintas magnéticas:

- La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:
- Temperatura: 4°C a 32° C Humedad Relativa: 20% a 80 %
- El ambiente debe contar con aire acondicionado.
- Las cintas deben colocarse en estantes o armarios adecuados.
- Deberá mantenerse alejados de los campos magnéticos.
- Se les debe dar un mantenimiento preventivo en forma periódica a fin de desmagnetizar impurezas que se hayan registrado sobre ellas.

b) **Cartuchos**

- Las recomendaciones para el buen mantenimiento de los cartuchos:
- La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:
- Temperatura: 16° C a mas Humedad Relativa: 20% a 80%.
- La temperatura interna del Drive puede oscilar entre:5° Ca $5° C.
- Deben ser guardados dentro de su caja de plástico.

- Deben mantenerse alejados de campos magnéticos.

14.5 Recomendaciones para el Mantenimiento de los Discos Duros.

Las recomendaciones para el buen mantenimiento de los discos duros:

- Aunque él. conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.
- La computadora debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.
- Se debe evitar que la computadora se coloque en zonas donde haya acumulación de calor. Esta es una de las más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.
- No se debe moverla CPU conteniendo al disco duro cuando este encendido, porque los cabezales de lectura – escritura pueden dañar al disco.
- Una de las medidas más importantes es este aspecto, es hacer que la gente tome conciencia de lo importante que es de cuidar un computador.

14.6 Recomendaciones Respecto a los Monitores.

Las recomendaciones para el buen mantenimiento de monitores son:

- La forma fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección.
- Se recomienda sentarse por lo menos a 60•cm. De la pantalla.
- No solo esto reducirá su exposición a las emisiones (que se disipan a una
- razón proporcional al cuadrado de la distancia), sino que ayuda a reducir el esfuerzo visual.
- También manténgase por lo menos 1 m. o 1.20 m del monitor de su vecino,
- ya que la mayoría de los monitores (antiguos) producen mas emisiones por
- detrás, que por delante.
- Finalmente apague su monitor cuando no lo esté usando.

14.7 Recomendaciones para el cuidado del equipo de Cómputo.

- Teclado. Mantener fuera del teclado grapas y clips, pues, de insertarse entre las teclas, puede causar un cruce de función.
- Unidad Central de Procesamiento. Mantener la parte posterior del CPU liberado en por lo menos 10 cm. Para asegurar así una ventilación mínima adecuada.
- Mouse. Poner debajo del Mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de este.
- Protector de pantalla. Estos sirven para evitar la radiación de las pantallas antiguas a color que causan irritación a los ojos.
- Impresora. El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel.

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

15 CONCLUCIONES FINALES

- Finalmente con relación al plan de contingencias Informático realizar un reporte de los daños, y documentarlas actividades desarrolladas durante todo el proceso de la contingencia.
- Cuantificar y valorizar las perdidas, que permitan tomar mejores decisiones respecto a la seguridad de la información y la continuidad de los servicios informáticos.
- Que el personal encargado del área de contingencia se reúna para analizar el plan de continencias y realizar las modificaciones correspondientes, así como las funciones o acciones del personal de contingencias.

16 ANEXOS

16.1 Formato Nº 1: EVALUACION DE DAÑOS

NOTA: La información sobre costos de los daños se anotara siempre que sea posible y en base a conocimientos técnicos para una estimación adecuada.

I INFORMACION GENERAL

Dependencia	Unidad Orgánica	Equipo de Trabajo

II FECHA DE INGRESO DE LOS DATOS

Día	Mes	Año

III EVENTO QUE OCACIONO LA EMERGENCIA O EL DESASTRE

IV FECHA Y HORA DE INICIO

Día	Mes	Año
Hora		

V DESCRIPCION DE LA EMERGENCIA O DEL DESASTRE

VI USUARIOS AFECTADOS

VII DAÑOS DE EQUIPAMIENTO

Tipo	Destruido	Inoperativo	Afectada	Costo S/. Aproximado
Servidor				
PC				
Laptop				
Impresora				
Escáner				
Proyector Multimedia				
Plotter				
TOTAL				

VIII DAÑOS A LA INFRAESTRUCTURA DE RED/COMUNICACIONES

RED LAN			
Tipo	Unidades Destruidas Inoperativas	Costo S/. Aproximado	Detallar ubicación Del área afectada
Switch			
Router			
Modem			
Central Telefónica			
TOTAL			

COMUNICACIONES – RED MAN/WAN			
	Zona/Dependencia	Costo S/. (Aproximado)	Detallar ubicación Zonal/Área afectada
Cableado LAN			
Enlace (Puente inalámbrico)			
Servicio de Prove de Internet			
TOTAL			

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

IX DAÑOS A LOS SISTEMAS DE INFORMACION (SOFTWARE)

APLICACIONES WEB			
Modulo	Afectado		
	Archivo Binario, Ejecutable o Script (Porcentaje)	Base de Datos (Porcentaje)	Ultimo acceso o actualización

APLICACIONES DE ESCRITORIO WINDOWS – DE CONSULTA			
Modulo	Afectado		
	Archivo Binario, Ejecutable o Script (Porcentaje)	Base de Datos (Tablas)	Ultimo acceso o actualización
Sistema APIMONS			
Sistema de Contabilidad			
Sistema de Tesorería			
Sistema de Personal (SISPER)			
Sistema de Administración Financiera (SIAF)			
Software de Inventario Mobiliario Institucional (SIMI)			
Sistema de Tramite Documentario (STD)			
Sistema de Gestión de Inmobiliaria (SGI)			
Sistema de Gestión de Abastecimiento (SGA)			

APLICACIONESD PROPORCIONADAS POR TERCEROS			
MODULO	Afectado		
	Archivo Binario, Ejecutable o Script (Porcentaje)	Base de Datos (Tabla)	Ultimo acceso o actualización
ADCOA			
SAGU			
STD			
Otro (Especifique)			

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

CARTILLA PARA EL LLENADO DEL FORMATO 1

DEFINICIONES:

Afectado:
Persona, animal, territorio o infraestructura que sufre perturbación en su ambiente por efectos de un fenómeno. Puede requerir de apoyo inmediato para eliminar o reducir las causas de la perturbación para la continuación de su actividad normal.

Peligro:
La probabilidad de ocurrencia de un fenómeno natural o tecnológico potencialmente dañino para un periodo específico y una localidad o zona conocida.

Fenómeno:
Todo lo que ocurre en la naturaleza que puede ser percibidos por los sentidos y ser objeto del conocimiento, además, del fenómeno natural existe el tecnológico o inducido por la actividad del hombre.

Emergencia:
Estado de daños sobre la vida, el patrimonio y el medio ambiente ocasionados por la ocurrencia de un fenómeno natural o tecnológico que altera el normal desenvolvimiento de las actividades de la zona afectada.

Desastre:
Es una interrupción grave en el funcionamiento de un servicio causando pérdidas de consideración a nivel humano, material o ambiental.

Colapsado:
Instalación en escombros.

DESARROLLO

Formato N° 01: Evaluación de Daños

I INFORMACION GENERAL

Se registran los datos referentes a la ubicación en la Estructura Orgánica de la Institución del Área afectada.

II FECHA DE INGRESO DE LOS DATOS

Se registra la fecha exacta del llenado del formato

III EVENTO QUE OCACIONO LA EMERGENCIA O EL DESASTRE

Se registra el fenómeno natural o tecnológico que ocasionó la emergencia o el desastre.
Ejemplo: Lluvias, sismo, incendio, etc.

IV FECHA Y HORA DE INICIO

Se registra la fecha y hora que ocurrió el desastre.

V DESCRIPCION DE LA EMERGENCIA O EL DESATRE

Se describe brevemente el comportamiento de la emergencia o el desastre, resaltando en forma General los daños ocasionados.

VI USUARIOS AFECTADOS

Se registra en número de usuario y las áreas afectadas.

VII DAÑOS AL EQUIPAMIENTO

Este componente cuenta con 06 filas: Servidor, PC, Laptop, Impresora, Escáner, Proyector Multimedia, Plotter, en los cuales se registra el nivel de los daños en los bienes señalados debido a la intensidad del desastre.

Destruido: Instalación en escombros, equipo destruido, con muestras visibles de daño físico.

Inoperativo: Instalación severamente dañada, equipo inoperativo y que requiere de reparación.

Afectada: Instalación ligeramente afectada, equipo que a simple vista no muestra daño físico pero cuyo funcionamiento se vio afectado por el evento.

Costo: Se registra el costo aproximado en soles, de acuerdo al tipo de daño.

VIII DAÑOS A LA INFRAESTRUCTURA DE RED/COMUNICACIONES

Este componente cuenta con cuatro filas: Switch, Router Modem y Central telefónica, en los cuales se registra la cantidad de unidades destruidas o inoperativas (en razón que su reparación o reemplazo dependerá de un tercero.

Costo (aproximado): Se registra el costo del total de los indicadores:

Detallar ubicación del área afectada: Se describe brevemente la ubicación física: IDF, Dependencia, Área, etc. Donde se encuentra ubicado el equipo destruido o inoperativo.

IX DAÑOS EN LOS SISTEMAS DE INFORMACION (SOFTWARE)

Aquí se considera únicamente el comprobante software de los Sistemas de Información, PARA LO CUAL SE HA ELABORADO UNA TABLA QUE INCLUYE AL Sistema Informático de Gestión Administrativa – SIGA y los módulos que lo conforman. Así también se han elaborado otras cinco tablas que contienen: Otras Aplicaciones Web, Aplicaciones de escritorio Windows en Producción, Aplicaciones de Escritorio Windows de >Consulta, Aplicaciones Proporcionadas por Terceros y otro Software Comercial, lo cual permitirá identificar rápidamente los aplicativos durante el registro de los daños.

Scripts – Archivo Binario, Ejecutable o Script (Porcentaje): Se registra una cantidad porcentual estimada de afectación de los Archivos Binarios, Ejecutables o Scripts del modulo o aplicación correspondiente.

Base de Datos (Porcentaje): Se registra una cantidad porcentual estimada de afectación en la base de datos respecto Modulo, Aplicación o Software a la que se hace referencia.

Ultimo acceso o actualización: En la fecha del último ingreso a la aplicación o actualización en la información a través del mencionado Modulo, Aplicación o Software a la que se hace referencia.

X DAÑOS AL SISTEMA ELECTRICO

Este componente cuenta con dos filas: Red de energía eléctrica interna (al interior de las oficinas) y Red de energía eléctrica troncal (en la parte que conectan los diferentes sectores del complejo, Incluida la subestación y su enlace con el cableado publico), en los cuales se registra la cantidad en metros lineales de cables que han colapsado o que se han visto afectadas.

Colapsado Red de Cables: Se escribe la cantidad de metros lineales de la Red de Cables que han interrumpido el funcionamiento del servicio.

Afectado Red de Cables: Se escribe la cantidad de metros lineales de la Red de Cables que hacen que el servicio se brinde pero con ciertas deficiencias o con interrupciones breves.

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA Oficina de Informática

XI OBSERVACIONES

Se registra brevemente las observaciones que se puedan efectuar sobre el desarrollo de la evaluación de los daños o alguna eventualidad.

XII RECOMENDACIONES

Se registra brevemente las recomendaciones que se pueden efectuar para mejorar la evaluación de daños y sobre prioridades en las necesidades.