MUNICIPALIDAD DISTRITAL DE SAN SEBASTIAN
SUB GERENCIA DE PLANEAMIENTO
- CUSCO -

MUNICIPALIDAD DISTRITAL DE SAN SEBASTIAN
OTSI
CUSCO

PLAN DE CONTINGENCIAS INFORMATICO

Municipalidad Distrital de San Sebastián - OTSI

Descripción breve

[Dibujar su lector con un resumen de la participación. Normalmente es un breve resumen del documento.
Cuando esté listo para agregar contenido, haga clic aquí y empiece a escribir.]

PROVEIDO N° ..... GM-MUSS
San Sebastián ..... de ..... del 2021
PASE A .....
PARA .....
.....
.....
ATTE
.....
GERENTE MUNICIPAL
(2019-2022)

OTSI
otsi@munisansebastian.gob.pe

PRESENTACION

La información es uno de los más importantes activos que posee toda institución la cual se genera en sus acciones y diferentes ámbitos, La Oficina de Tecnología Sistemas Informáticos, de la Municipalidad Distrital de San Sebastián, consciente de esta premisa puede advertir que se debe adoptar medidas de seguridad para la información y así mismo estar preparados para afrontar contingencias y diversos desastres, como por ejemplo; virus informáticos, sismos, inundaciones, personas mal intencionadas, cortes del fluido eléctrico, instalaciones eléctricas y de transmisión de datos implementadas al intemperie, usuarios con escaso conocimiento informático, uso de pendrives sin antes escanear con el antivirus correspondiente, escaso personal profesional y técnico, etc. por lo que el riesgo de sufrir situaciones críticas es muy alto, más aún, teniendo en cuenta el nivel sociocultural y económico de esta entidad, los cuales determinan una alta vulnerabilidad a la información computarizada municipal.

La Oficina de Tecnología Sistemas Informáticos de la MDSS, tiene como propósito el de proteger la información, asegurando su procesamiento y desarrollo. Es por ello que presentamos el Plan de Contingencia de Sistemas de Información, diseñado para el desarrollo y ejecución de los objetivos de cada año, la ejecución del Plan de Contingencias permitirá prevenir y menguar cualquier problema y/o desastre relacionado con la información, software y hardware, así como con los suministros informáticos y el personal de la municipalidad.

Actualmente, los profesionales y técnicos de la informática tienen como una de sus principales actividades y ocupaciones la seguridad de la información, lo cual constituye una base y respaldo a las funciones institucionales realizadas a través de los años. En la actualidad los Sistemas Informáticos facilitan de sobre manera las tareas que se desarrollan en la ejecución de los diferentes procesos administrativos, logísticos, financieros, de planeamiento y de servicios.

El personal de OTSI, responsables del servicio informático de la municipalidad están obligados a hacer de conocimiento y explicar con lenguaje entendible a los gerentes y/o personal municipal las posibles consecuencias que la seguridad insuficiente o inexistente pueda acarrear; de esa manera proponer y poner a consideración las medidas de seguridad inmediatas a mediano plazo, que han de tomarse en cuenta para prevenir los desastres que pueda provocar el colapso de los sistemas informáticos.

INTRODUCCION

Conocido es que toda organización es vulnerable a las fallas o caídas de los sistemas informáticos poniendo en riesgo el normal funcionamiento de las diversas actividades que realiza tanto en bienes como en servicios, como es el caso de la municipalidad, ya que la paralización de los servicios informáticos internos y externos de esta municipalidad, originaría por falta de prevención, un gran malestar a toda la población contribuyente, a trabajadores y directivos municipales.

El Plan de Contingencia es el instrumento de gestión para el buen manejo de las Tecnologías de la Información y de las Comunicaciones. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la institución. Así mismo, este plan de contingencias sigue el conocido ciclo de vida iterativo, "planifica-actúa-comprueba-corrige". Surge de un análisis de riesgos, donde entre otras amenazas, se identifican aquellas que afectan a la continuidad de la operación de la entidad.

El Plan de Contingencia permitirá mantener la contingencia operativa frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma, los usuarios y clientes, deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución adecuada.

El Plan de Contingencia debe involucrar a los actores relevantes. Este plan de trabajo considera evaluar las situaciones de riesgo y definir las tareas orientadas a reducir dichos riesgos.

INDICE

PLAN DE CONTINGENCIA INFORMATICO

CAPITULO I

GENERALIDADES Y CONCEPTOS PREVIOS

1. GENERALIDADES

1.1. OBJETIVO.

1.1.1. OBJETIVO GENERAL.

Contar con un Plan de Contingencias actualizado, que permita la continuidad en los procedimientos informáticos de la Oficina de Tecnología y Sistemas Informáticos, así como disminuir las fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; manteniendo la calidad en los servicios que brinda esta Oficina.

1.1.2. OBJETIVO ESPECIFICO.

a. Contar con documentación práctica y actualizada que garantice a la MDSS la continuidad de las operaciones de los sistemas informáticos sin sufrir paralizaciones o perdidas relevantes.
b. Identificar y analizar riesgos posibles que pueden afectar las operaciones y procesos informáticos de la institución.
c. Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que ésta no exceda las 24 horas.
d. Contar con personal debidamente capacitado y organizado para afrontar adecuadamente las contingencias que puedan presentarse en las actividades de la MDSS.

1.2. FINALIDAD.

- Garantizar que los procesos críticos de la MDSS continúen funcionando a pesar de una posible falla en los sistemas computarizados. Es decir, un plan que le permite a la Institución seguir operando, aunque sea al mínimo.
- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los sistemas de información
- Definir acciones a ejecutar en caso de fallas de los elementos que componen un sistema de información.

1.3. BASE LEGAL.

- DL. N° 604, Ley de Organización y Funciones del INEI.
- DS. N° 018-91-PMC, Reglamento de Organización y Funciones del INEI.
- RJ. N° 340-94-INEI, Normas Técnicas para el procesamiento y respaldo de la información que se procesa en entidades del Estado.
- RJ. N° 076-95-INEI, Recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.
- RJ. N° 090-95-INEI, Recomendaciones Técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.
- Ley N° 27972 - Ley Orgánica de Municipalidades.
- Resolución Ministerial N° 04-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición", en todas las entidades integrantes del Sistema Nacional de Informática. Quedando derogada la Resolución Ministerial N° 129-2012-PCM.

- Decreto Supremo N° 066-2011-PCM que aprueba el "Plan de Desarrollo de la Sociedad de la información en el Perú - La Agenda Digital Peruana 2.0", y que en su Objetivo N° 7, establece la necesidad de promover una Administración Pública de calidad orientada a la población, y la necesidad de contar con una Estrategia Nacional de Ciberseguridad, con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos Informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros.
- Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI Tecnologías de la Información, Código de Buenas Prácticas para la Gestión de Seguridad de la Información 2da edición en todas las entidades integrantes del Sistema Nacional de Informática.
- Decreto Supremo N° 031-2006-PCM, que aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana".
- Resolución Ministerial No 274-2006-PCM, que aprueba la "Estrategia Nacional de Gobierno Electrónico".
- Resolución de Contraloría General N° 320-2006-CG, que aprueba las "Normas de Control Interno", que son de aplicación a las entidades del Sector Público.

1.4. ALCANCE.

El presente Plan de Contingencia es de aplicación y cumplimiento obligatorio en las unidades orgánicas siguientes:

- Oficina de Tecnología y Sistemas Informáticos.
- Gerencias Centrales, Gerencias de apoyo, de línea y órganos de asesoramiento y de control.

1.5. META.

Potenciar el nivel informático de la Oficina de Tecnología y Sistemas Informáticos de la MDSS, y además las funciones cotidianas informáticas, haciéndolas seguras y consistentes, logrando con ello su buen desarrollo y la optimización de resultados

1.6. DEFINICIONES.

¿Qué es un sistema de información?

Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos formarán parte de alguna de las siguientes categorías: Personas; Datos; Actividades o técnicas de trabajo; Recursos materiales en general (generalmente recursos informáticos y de comunicación, aunque no necesariamente).

Un Sistema Informático utiliza ordenadores para almacenar los datos de una organización y ponerlos a disposición de su personal. Pueden ser tan simples como en el que una persona tiene una computadora y le introduce datos, los datos pueden ser registros simples como ventas diarias, se produce una entrada por cada venta.

Sin embargo, la mayor parte de los sistemas son más complejos que el enunciado anteriormente. Normalmente una organización tiene más de un sistema informático y redes de computadoras para soportar las diferentes funciones de la organización, ya sean servicios, ventas, recursos humanos, contabilidad, producción, inventario, etc.

Los sistemas de información tienen muchas cosas en común. La mayoría de ellos están formados por personas, equipos y procedimientos. Al conjugar una serie de elementos

como hombres y computadoras se hace imprescindible tomar medidas que nos permitan una continuidad en la operatividad de los sistemas para no ver afectados los objetivos de las mismas y no perder la inversión de costos, tiempo y beneficio.

¿Qué es un Plan de Contingencia?

Un Plan de Contingencias es una herramienta estratégica planificada con una serie de procedimientos que nos facilitan u orientan a tener una solución alternativa y nos permite restituir rápidamente los servicios de la organización ante la eventualidad que pueda paralizar los servicios, ya sea de forma parcial o total, es decir, un plan que le permite a su negocio u organización, seguir operando, aunque sea de forma limitada.

Características principales de un Plan de Contingencia

- **Amplio.** - Porque considera a todos los componentes de los procesos de una institución u organización.
- **Abierto en el tiempo**. - Para dar respuesta permanente a cualquier tipo de incidencias.
- **Participativo.** - Porque se pretende que intervenga todos los agentes, instituciones o agrupaciones que estén implicados de una u otra forma en el servicio.
- **Eminentemente práctico.** - Ya que fija objetivos concretos y establece los medios y los plazos.

La vigencia del plan será hasta que los procesos a los que suple estén nuevamente operativos.

Acciones a ser consideradas

- **Antes**, como hacer un plan de respaldo o de prevención para mitigar los incidentes.
- **Durante**, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
- **Después**, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

El Plan de Contingencia permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. El término "incidente" en este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático en la MDSS.

Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan. El plan de prevención es la parte principal del Plan de Contingencia de Sistemas de Información porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible. Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

Plan de Recuperación

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia. Todo Plan de Contingencia de Sistemas de Información debe tener un carácter recursivo que permita retroalimentar y mejorar continuamente los planes en cada una de las etapas descritas, logrando así tener un documento dinámico.

Plan de Pruebas

El Plan de Pruebas, será presentado a la Gerencia Municipal de la MDSS, para su aprobación previa a su implementación. El resultado de las pruebas efectuadas será presentado igualmente para su conformidad. Las pruebas relacionadas a este plan, se ejecutaría trimestralmente, con el fin de evaluar la preparación de la organización ante la ocurrencia de un siniestro y realizar los ajustes necesarios.

CAPITULO II.

DESARROLLO DE LAS FASES METOLOLOGICAS, ACTIVIDADES, ESTREGIAS.

2. MARCO METODOLÓGICO

Los planes de contingencia se organizan para que las instituciones y empresas puedan prevenir fallas o accidentes en sus operaciones diarias, permitiéndoles continuar activas, en tanto a la provisión de bienes y servicios, en el caso de que algún componente presente cualquier tipo de problemas que condicione el correcto funcionamiento de sus equipos tecnológicos, aplicaciones informáticas y otros sistemas críticos, lo cual indica que la Oficina de Tecnología y Sistemas Informáticos debe poner en marcha el mencionado plan para la recuperación de la Entidad.

Se debe tener presente que mucho dependerá de la infraestructura de la municipalidad y de los servicios que ésta ofrezca para determinar un modelo de desarrollo de plan, **no existe un modelo único para todos,** lo que se intenta es brindar los puntos más importantes a tener en cuenta.

La metodología empleada para el desarrollo y aplicación del plan de contingencias de los sistemas de información, ha sido desarrollada por INEI, en base a la experiencia lograda en el desarrollo de planes de contingencia del año 2001.

La presente metodología se podría resumir en **ocho fases** de la siguiente manera:

i Fase 1 Planificación: preparación y aprobación de esfuerzos y costos.
ii Fase 2 Identificación de riesgos: funciones y flujos del proceso de la empresa.
iii Fase 3 Identificación de soluciones: evaluación de riesgos de fallas o interrupciones.
iv Fase 4 Estrategias: otras opciones, soluciones alternativas, procedimientos manuales.
v Fase 5 Documentación del proceso: creación de un manual del proceso.
vi Fase 6 Realización de pruebas: selección de casos, soluciones que podrían funcionar.
vii Fase 7 Implementación: creación de soluciones requeridas, documentación de casos.
viii Fase 8 Monitoreo: probar nuevas soluciones o validar los casos.

2.1. FASE 1 - PLANIFICACION

La fase de planificación es la etapa donde se define y prepara el esfuerzo de planificación de contingencia/continuidad los servicios informáticos

2.1.1. Diagnóstico

La Oficina de Tecnología y Sistemas Informáticos de la Municipalidad Distrital de San Sebastián hace una revisión de administración de los riesgos y, no existe un Plan de Contingencias. Se ha observado que no existe las normas, procedimientos y controles que cubren algunos aspectos de la seguridad de la información, que carece en general de una metodología, guía o marco de trabajo que ayude a la identificación de riesgos y determinación de controles para mitigar los mismos.

Dentro de los distintos aspectos a considerar en la seguridad, es necesario elaborar Políticas de Seguridad de la Información y una Clasificación de Seguridad de los Activos de Información de la Municipalidad. Cabe mencionar que no se ha encontrado la existencia de controles, en el caso de la seguridad lógica, sobre los accesos a los sistemas de información, así como procedimientos técnicos establecidos para el otorgamiento de dichos accesos.

Sin embargo, existen procesos que no obedecen a una definición previa de una Política de Seguridad ni de una evaluación de riesgos de seguridad de la información a nivel de toda la Municipalidad. Los controles establecidos a la fecha son productos de evaluaciones particulares efectuadas por las áreas involucradas o bajo cuyo ámbito de responsabilidad recae cierto aspecto de la seguridad.

2.1.2. Talento y Humano Recursos Institucionales.

El presente Plan de Contingencia requiere como respaldo contar con algunos requisitos para la puesta en marcha:

2.1.2.1. Talento Humano.

Están dados por las personas participantes directa e indirectamente en el desarrollo del Plan, las cuales en un primer momento será el personal de la OTSI con que cuenta la MDSS, quienes definirán los procedimientos para poner en operación el Plan de Contingencias.

Tenemos luego a los Gerentes que al comprender la importancia y urgencia de la aplicación de este plan habrán de apoyar las propuestas que dan base a la ejecución del plan de contingencias, y han de hacer denominador común para su aplicación. Por último, las personas de diferentes áreas y oficinas de la MDSS que servirán de nexo para la captura de información y definición de tareas del plan.

2.1.2.2. Materiales

Todas las herramientas de soporte, material de escritorio, computadores, equipos, insumos informáticos, útiles de escritorio, necesario para llevar a cabo el plan.

2.1.2.3. Financieros

Los recursos financieros con que se requiere contar para la aplicación del presente Plan de Contingencia, en acuerdo con la parte del plan de la OTSI fueron indicados en el Cuadro de Necesidades 2021.

2.1.2.4. Entrenamiento

El personal participante será entrenado para la aplicación correcta del Plan y para obtener el máximo provecho de acuerdo a la función que han de cumplir como parte conformante del plan.

2.1.2.5. Responsabilidad

La alta dirección (gerentes) habrá de ejercer la función de control y asegurará que las tareas desarrolladas, sean cumplidas de acuerdo a los planteamientos y objetivos del plan.

Los Planes de Contingencia se organizan para que las instituciones puedan prevenir fallas o accidentes en sus operaciones diarias y les permitan seguir activas, en la provisión de servicios o productos, en el caso de que algún componente sufra algún tipo de problema, que condicione el correcto funcionamiento de sus equipos tecnológicos, aplicaciones informáticas y otros sistemas críticos.

2.1.3. Servicios y/o Bienes Producidos

La Municipalidad Distrital de San Sebastián es una institución que se encarga de brindar servicios a los vecinos de la ciudad del Cusco, distrito de San Sebastián:

- promover la participación vecinal.
- Fortalecer la seguridad ciudadana.
- Mantener los parques y jardines.
- Garantizar el control sanitario.
- Conservar el medio ambiente.
- Promover el bienestar social.
- Promover la modernización tecnológica
- Fomentar la cultura, el deporte y el turismo.
- Proveer limpieza pública.
- Mantener la infraestructura vial.
- Administrar el Registro Civil.

Entre otros, para cumplir con las disposiciones legales vigentes y poder brindar bienestar y desarrollo a la comunidad.

2.1.4. Inventario de recursos informáticos

2.1.4.1. Equipos informáticos diversos

PROCESADOR	CANTIDAD
Pentium (I, II, III, IV)	2
Core 2 Quad	4
Core I3	19
Core I5	63
Core I7	160
AMD	16
LAPTOP	60
Servidor de Rentas	1
servidor SIAF	1
servidor SIADEG	1
Servidor SGD	1
Servidor de SIGA	1
Servidor de Registro de Asistencia	1
Servidor de Caja	1
Servidor DSPlanillas	1
Fotocopiador	26
Escaner	6
Impresora	50
Impresora Multifuncional	200
Proyector	19
TOTAL GENERAL	633

2.1.4.2. Software Utilizado.

El Software utilizado en la MDSS se muestra en el siguiente cuadro:

N°	Nº	SOFTWARE
1	**Sistemas Operativos**	Windows XP - 32 bits
		Windows 7 - 32 bits

		Windows 7 - 64 bits
		Windows 8 - 64 bits
		Win 10 - 32 bits
		Win 10 - 64 bits
		Windows Server 2008
		Windows Server 2012
2	**Motores de Base de Datos**	SQL Server 2008
		SQL Server 2012
		MySQL Workbench
		Postgresql
3	**De Oficina**	Paquete de Office 2007, 2010,2013, 2016
4	**Antivirus**	Nod 32 V 7.1

2.1.4.3. Aplicativos Informáticos.

N°	SISTEMA	DESCRIPCION	**RESPONSABLE FUNCIONAL**
1	Reporte de Cuenta Predial Formato Web	Modulo Web para la consulta de tu estado de deuda predial	Sub Gerencia de Recaudacion Tributaria
2	Caja Online Formato Web	Software que permite operaciones de flujo monetario	Sub Gerencia de Tesoreria
3	Limpieza Online Formato web	Software que permite operaciones de consulta para la facturacion del servicio de limpieza publica	Sub Gerencia de Residuos Solidos
4	Tramite Documentario	Software de mesa de partes virtual	en todas las areas
5	SIADEG	Modulo Gubernamental, quienes pueden llenar sus registros de logistica y alamacenes	Sub Gerencia de Abastecimiento
6	Huamán Poma de Ayala	Sistema de administración tributaria	Gerencia de Administración Tributaria
7	DSPLANILLAS	Software para la gestión del personal	Gerencia de Recursos Humanos
8	SIGA	Sistema Integrado de Gestión Administrativa	Todas las Unidades Orgánicas.
9	SIAF	Sistema Informático de Administración Financiera	Administración Logística, tesorería Contabilidad, Presupuesto
10	Roundcube	Correo Institucional	Todas las Unidades Orgánicas

2.1.5. Análisis de riesgos.

RIESGO	Factor de Riesgo				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Incendio					x
Inundación		x			
Robo Común					x
Vandalismo, daño de equipos y archivos					x
Fallas en los equipos, daño de archivos					x
Equivocaciones, Daño de archivos			x		
Virus, daño de equipos y archivos					x
Terremotos, daños de equipos y archivos.				x	
Acceso no autorizado, filtración de información.					x
Robo de datos.					x
Fraude, alteración de información.				x	
Desastre total					x

2.2. FASE 2 Y 3 – IDENTIFICACIÓN DE RIESGOS Y SOLUCIONES.

2.2.1. Plan de reducción de riesgos (Análisis de Riesgos)

El Plan de reducción de riesgos busca minimizar las fallas generadas por diversos motivos a partir del análisis de los proyectos desarrollados por el Plan Operativo Institucional (POI).

2.2.2. Evaluación de Riesgos Potenciales y no Potenciales

Todos los sistemas informáticos de la Municipalidad distrital de San Sebastián están expuestos a grandes riesgos por pérdida de información técnica incluso el canibalismo de las computadoras, virus informático, etc. Así como el cableado eléctrico, telefonía y redes de transmisión de datos no prestan las garantías del caso.

Se presenta una lista detallada, previa evaluación de los posibles riesgos potenciales y no potenciales que podrían presentarse en la Oficina de Tecnología y Sistemas Informáticos y otras áreas de la Municipalidad Distrital de San Sebastián, asimismo se incluye una solución para cada caso:

2.2.2.1. Riesgos Potenciales

Destrucción total o parcial de la Oficina de Tecnología y Sistemas Informáticos - OTSI, por desastres naturales o causados por la negligencia del hombre: inundaciones, terremotos, incendios, etc.

Solución:

- Mantener cubierto el stock de material técnico para todo el año, (CDs, DVDs, Discos Duros externos de gran capacidad, memorias USB, otros insumos acordes a la tecnología existente).
- Realizar copias de seguridad de los diversos sistemas informático diariamente, debiendo preservar una copia en caja fuerte y otra en alguna entidad de almacenamiento de la localidad.

- Actualizar las copias de seguridad de la información fuente de los sistemas informáticos en forma semanal o quincenal y de las bases de datos en forma diaria o semanal según corresponda.
- Realizar convenios con empresas del medio para que nos alquilen equipos de cómputo en casos de emergencia.
- Proceder a recuperar la información a partir de los backups que se encuentran almacenados.

Apagones del fluido eléctrico desde la misma planta de servicios eléctricos u otras averías externas.

Solución:
Contar con un generador de luz y un UPS en óptimas condiciones, para poder continuar brindando el servicio informático a los contribuyentes, en caso de pérdida de información se recuperará a partir de los backups.

Cableado eléctrico, tendido a la intemperie por los techos y paredes de este local, lo cual genera interferencias en la transmisión de datos

Solución:
Revisión y evaluación total del actual sistema eléctrico del municipio, por parte del personal electricista de esta comuna y proponer una inmediata solución, recomendándose que el nuevo tendido de cable se implemente en el interior de las estructuras del edificio o en su defecto mediante canaletas para protegerlo y evitar las interferencias eléctricas.

Pérdida de Información automatizada (robos), por personas mal intencionadas.

Solución:
- Restaurar la información a partir de los backups existentes en los archivos, caja fuerte o entidades de almacenamiento.
- Iniciar una investigación interna exhaustiva a los administradores de servidores y/o operadores de PC.
- Formular la denuncia correspondiente ante el órgano policial correspondiente a fin de deslindar responsabilidades.

Contagio de la Información automatizada (virus informático), transmitido por el mal uso de Internet u otros medios de almacenamiento que transporte información.

Solución:
- Restaurar la información a partir de los backups existentes en los archivos, caja fuerte o entidades de almacenamiento.
- Identificar a los usuarios que generan este daño innecesario a sus equipos informáticos, para capacitarlos en el uso del Software Antivirus.

Huelgas de los servidores municipales (toma de local).
Solución:
- El personal técnico y/o profesional no debe estar involucrado en las huelgas debido a que el servicio que realiza está orientado a brindar soporte tecnológico a los administrados de esta comuna.

- Se debe gestionar ante la superioridad una Resolución Municipal que garantice la integridad y el bienestar del personal técnico y/o profesional que brinda soporte tecnológico.

2.2.2.2. Riesgos no Potenciales

Cableado de redes para transmisión de datos instaladas a la intemperie, expuestas a los problemas del medio ambiente y otros

Solución:
Revisión y evaluación del actual sistema de cableado de redes, por parte del personal técnico y/o profesional de Redes y Comunicaciones de esta gerencia, quienes deberán proponer una solución que permita brindar seguridad en la transmisión de datos, recomendándose que el tendido de cable se haga con canaleta o empotrado para protegerlo y evitar las interferencias, trabajo que debe estar supervisado por el despacho de la Oficina de Tecnología y Sistemas Informáticos.

Cableado de telefonía, tendido a la intemperie expuesto a los problemas del medio ambiente y otros.

Solución:
Revisión y evaluación total del actual cableado telefónico del municipio, la empresa proveedora del servicio de telefonía debe proponer y ejecutar una solución inmediata, recomendándose el uso de nuevas tecnologías en comunicaciones e implementar una Central telefónica IP.

Escaso material técnico para resguardo de información (Discos duros externos, CD's, DVD's, pendrives, etc.)

Solución:
El comité de Contingencias debe exigir la adquisición de repuestos, herramientas y accesorios informáticos para prevenir los desastres, así como para brindar el mantenimiento preventivo y correctivo de los diversos equipos del parque informático de la MDSS, por otro lado, es necesario que también sea adquirido el material y herramientas

Ambiente inadecuado para realizar las funciones asignadas al personal de las áreas funcionales de la OTSI

Solución:
- Gestionar ante la superioridad un ambiente exclusivo para reparación y mantenimiento de equipos de cómputo.
- Contratar un Técnico Electrónico en reparación de equipos servidores de datos, impresoras, monitores, plotters.
- Comunicar a todos los usuarios de la MDSS que presenten inconvenientes con el normal funcionamiento de su PC que se comuniquen y remitan sus equipos al Área de Soporte Técnico de la OTSI, los cuales serán atendidos por prioridad o en función a la existencia de repuestos.

Software Informático Municipal sin control, es decir sin inventario detallado que permita la rápida recuperación ante un desastre

Solución:

- El personal asignado a Desarrollo de Sistemas deberá hacer realizar el inventario detallado de los sistemas informáticos municipales.
- Buscar, diseñar o adquirir un software que controle la situación real de cada sistema informático.
- Mantener actualizado el inventario de software en forma digital.

Equipos informáticos y/o información técnica sin seguro, poniendo en riesgo la tranquilidad de los usuarios por desastres imprevistos

Solución:

- Realizar un convenio con alguna una empresa de seguros con la finalidad asegurar los equipos de cómputo (Servidores de Bases de Datos) y los diversos sistemas informáticos, teniendo en cuenta que el valor de la información técnica es costoso y que en caso de perderse totalmente sólo se recupera empezando desde cero.

Distribución y asignación de equipos informáticos sin revisión de perfiles de usuario.

Solución:

Elaborar los perfiles de usuario estándar para los trabajadores que tienen asignados equipos informáticos, de esta manera se podrá distribuir y asignar equipos teniendo en cuenta las funciones y tareas que deban realizar. Evitando el mal uso y desperdicio de las capacidades tecnológicas que ofrecen los equipos informáticos.

Pozos a tierra sin mantenimiento

Solución:

Ejecutar el mantenimiento de los pozos a tierra con el apoyo del personal eléctrico de la Sub Gerencia de Obras Públicas y Convenios o contratar personal externo según cronograma de mantenimiento establecido por la OTSI.

Escaso personal con conocimiento en análisis y desarrollo de sistemas informáticos para brindar soporte al software municipal

Solución:

Se debe contratar personal profesional o técnicos con conocimiento en ingeniería de requerimientos, análisis de sistemas, modelamiento de software, metodologías de desarrollo de software, lenguajes de programación, arquitectura de aplicaciones, modelamiento de bases de datos, etc.

Escaso personal con conocimiento en mantenimiento predictivo, preventivo y correctivo de equipos de cómputo

Solución:

Se debe contratar personal profesional o técnico, o capacitar al personal permanente asignado a la OTSI, en mantenimiento predictivo, preventivo y correctivo de equipos de cómputo, en su defecto contratar los servicios de

una empresa particular que realice dicho trabajo, estableciendo ciertas condiciones de garantía.

Escaso personal con conocimiento en redes de computadoras, así como en administración de equipos de comunicación y servicios de red

Solución:

- Se debe contratar personal profesional o técnico, o capacitar al personal permanente asignado a la OTSI, en redes de computadoras, administración de equipos de comunicación, servicios de red, entre otros afines.
- Mantener actualizado un libro de ocurrencias en físico o virtual, el cual permita el registro de las incidencias suscitadas en la red o sala de servidores ubicada en la OTSI.

Sistemas Informáticos no documentados apropiadamente, imposibilitando su fácil mantenimiento

Solución:

- Toda la documentación fuente de los diversos sistemas informáticos deben encontrarse debidamente actualizados en formato digital en una biblioteca virtual.
- Todas las modificaciones realizadas al software deben ser registradas en una bitácora y control de versiones detallando las funciones actualizadas o cambios realizados.

Sistemas Informáticos sin autorización normativa de aplicación municipal

Solución:

Todo sistema informático desarrollado por la OTSI o adquirido por terceros o cedido en uso debe ser debidamente autorizado por Resolución de Gerencia Municipal, y debidamente ejecutada por las áreas usuarios y bajo la supervisión de la OTSI.

Relación desactualizada de usuarios con acceso a la red municipal

Solución:

- El acceso a la red municipal, así como el uso de los servicios y sistemas informáticos debe estar regulado y controlado por el administrador de conectividad y seguridad de la OTSI.
- El administrador de conectividad y seguridad, debe depurar a los usuarios de la red municipal semanalmente y en casos de despidos, termino de contrato, termino de designación, renuncia de, entre otros debe proceder inmediatamente, para lo cual debe buscar los canales de comunicación pertinentes.

No se cuenta con una central telefónica que canalice las llamadas para actos administrativos, atenciones al administrado y para servicio técnico

Solución:

Gestionar y priorizar la implementación de la central telefónica para facilitar la comunicación de los administrados con las áreas pertinentes, las cuales

brindan la información solicitada. Por otro lado, la central telefónica es un medio para integrar las diversas unidades orgánicas y funcionales de la MDSS facilitando la comunicación masiva.

Acceso a la Oficina de Tecnología y Sistemas Informáticos y Sala de Servidores sin control de cámaras de video ni control manual, poniendo en riesgo a la información almacenada física y digitalmente, suministros informáticos, repuestos y accesorios de cómputo, etc.

Solución:

- Es necesario implementar medidas de seguridad, controlando el ingreso de personas no autorizadas al ambiente de la OTSI mediante cámaras de video vigilancia o personal con asignación específica, para lo cual se debe solicitar la adquisición de estos implementos, así como la instalación y puesta en marcha por parte del personal de redes y comunicaciones o de Soporte Técnico de esta gerencia o mediante contratación del servicio especializado.
- El acceso físico al ambiente de la OTSI o sala de servidores debe ser limitado, el uso de llaves debe ser controlado y dado solo al personal que asumirá las responsabilidades de todos los implementos y recursos que esta gerencia tiene a disposición cuando sea necesario.
- Controlar el registro de labores asignadas fuera del horario de oficina, así como el personal que labora los fines de semana por su régimen laboral o por horario especial.
- Prohibir que cualquier tipo de persona, sea particular o servidor municipal ingrese con bolsas, paquetes y otros medios a la OTSI.
- El ingreso y salida de equipos computacionales, accesorios informáticos y otros materiales debe ser controlado estrictamente por el personal de Soporte Técnico, en caso de ausencia por comisión de servicio el gerente delegará estas funciones al personal idóneo, para que informe de las ocurrencias acaecidas.
- Mantener una bitácora de accesos a la sala de servidores, así como de los accesorios, repuestos y demás implementos prestados a otras oficinas.

Ambiente de la OTSI inadecuado, sin salvaguardar la integridad de los trabajadores asignados a esta gerencia

Solución:

Gestionar el acondicionamiento y/o implementación de un nuevo ambiente que brinda mayores facilidades al personal de la OTSI para el desenvolvimiento de sus funciones.

La Oficina de Bienes Patrimoniales de la MDSS, deberá realizar un inventario de bienes, remitir al depósito los que se encuentren inoperativos.

Atenciones técnicas solicitadas sin criterio técnico

Solución:

- Elaborar un sistema informático que canalice las atenciones técnicas solicitadas por el personal municipal con la finalidad de mantener un registro por fechas y prioridades de atención, mejorando el control de las mismas.

- Las atenciones realizadas deberán variar de acuerdo al orden de prioridad de las mismas.
- El personal de la MDSS deberá de requerir solo atenciones técnicas cuando estas sean de estricta necesidad laboral para las actividades que desempeñan como parte de su función, y no para realizar actividades personales o ajenas a la institución.

Personal municipal carece de conocimiento de las nuevas tecnologías en los diversos ámbitos como son hardware, software y redes de comunicaciones

Solución:

- Establecer convenios con diversas casas de estudio sean universitarias o institutos, con la finalidad que estas brinden facilidades económicas al personal de la MDSS y puedan prepararse adecuadamente en temas como ofimática, internet y redes sociales, diagramación y diseño gráfico, etc.
- La capacitación del personal deberá ser aprobado por la Gerencia de Recursos Humanos y la OTSI, e incorporado en los Planes Operativos Institucionales de cada unidad orgánica, ejecutándose según los calendarios establecidos y su presupuesto asignado.

Despido intempestivo del personal Técnico y Profesional contratado

Solución:

Evaluar el desempeño laboral del personal profesional y técnico contratado tales como:

- Analistas de Sistemas.
- Diseñadores de Sistema.
- Programadores.
- Digitadores.
- Administradores de Redes y Comunicaciones.
- Administrador de Conectividad y Seguridad.
- Oficial de Seguridad de la Información.
  Administrador Estadístico.
- Operador Estadístico.
- Mantenimiento PCs (Hardware).
- Mantenimiento de redes y Comunicaciones.

2.2.3. Plan de Recuperación de Desastres

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en la que la Oficina de Tecnología y Sistemas Informáticos. y otras áreas pudieran estar expuestas Los planes de trabajo serán probados fehacientemente, asimismo los procedimientos deberán ser de ejecución obligatoria y estarán involucrados todo el personal del municipio, específicamente las áreas que trabajan con sistemas informáticos municipales y otros sistemas, así como también se tendrá la aprobación de la máxima autoridad (Alcalde) mediante Resolución de Alcaldía o Acuerdo Municipal.

2.2.3.1. Actividades Previas al Desastre

Se considera actividades previas al desastre a todo evento organizado por el Comité de Contingencias (CC), con el fin de poder recuperar el servicio

Informático en su totalidad en menor tiempo posible. Entre las principales actividades podemos mencionar.

- Organización y salvado de la Información técnica
- Evaluación y mejoramiento de los equipos de cómputo
- Formación de equipos de trabajo

Las actividades generales se realizarán en base al plan de recuperación de desastres en 3 etapas:

Establecimiento del Plan de Acción

El establecimiento del plan de acción comprende una planificación estructurada de actividades que deben cumplirse durante un desastre, y que a continuación de detalla.

Sistemas de Información

La Oficina de Tecnología y Sistemas Informáticos deberá contar con un backup y una relación de todos los sistemas de información municipal, tanto fuentes como ejecutables y la Base de Datos, asimismo, software de fábrica de desarrollo, así como de gestión, lo cual permitirá la rápida identificación de la información, la relación debe contener:

a) Nombre del Sistema
b) Lenguaje o paquete con el que fue creado el sistema (programas que lo conforman tanto fuentes como ejecutables)
c) Área que genera la información base.
d) Áreas que utilizan la información del sistema
e) Volumen de los archivos que trabaja el sistema
f) Volumen de transacciones que maneja el sistema, diarias, semanales, mensuales
g) Equipamiento necesario para el manejo optimo del sistema
h) Fecha en que la información fue ingresada
i) Fecha de creación de los Sistemas
j) Fechas de adquisición del Software
k) Nivel de importancia estratégica que tiene la información del sistema para la institución y/o área
l) Actividades a realizar para restablecer el sistema de información

Equipos de cómputo

- Contar con un inventario total y actualizado de todos los equipos de cómputo.
- Gestionar pólizas de seguro comerciales para los equipos de cómputo (Servidores) como parte de protección de los mismos, pero haciendo la salvedad en el contrato, que, en casos de siniestros, la destrucción total del computador
- Debe ser repuesto por un equipo de las mismas características o mejor aún, según los nuevos avances de la tecnología siempre y cuando los valores estén considerados dentro los montos asegurados.
- Señalización o etiquetado de los computadores y redes de acuerdo a la Importancia de su contenido para la priorización en caso de evacuación. (usar colores)

Obtención y almacenamiento de los respaldos de información (backups)
En el presente manual quedan establecidos los procedimientos para la obtención de las copias de seguridad de toda la información técnica desarrollada por personal del municipio y adquirido a los distribuidores.

a. Backups de los todos los Sistemas Operativos
b. Backups del software base (Gestión, lenguajes de programación, paquetes de Diseño, etc.).
c. Backups de Sistemas Municipales (programas fuentes y objetos)
d. Backups de los datos (bases de datos, índices, tablas de validación, archivos de password y todo archivo necesario.
e. Backups de hardware quiere decir hacer convenios sobre hardware con proveedores o instituciones, para que cedan equipos de cómputo en alquiler o préstamos, si el caso lo amerita, con el fin de no paralizar la atención al público contribuyente.

Políticas (normas y procedimientos de backups)
En el presente ítem se establece los procedimientos, normas y determinación de responsabilidades en la obtención de los backups:

a. Periodicidad de cada tipo de backups
   - Información fuente de sistemas municipales salvar mensualmente, especialmente cuando hay modificaciones en los programas fuente.
   - Información ejecutable salvar mensualmente Información data (BD, archivos), salvar diariamente Información diversa, salvar diariamente.

b. Respaldo de información.
   - Como mínimo realizar los backups diarios en discos adicionales externos o virtuales, así como en memorias USB.

i Uso obligatorio de un formulario estándar para el registro y control de backups.
ii Almacenamiento de los backups en condiciones ambientales optimas recomendando que se utilice productos de calidad.
iii Reemplazo de los backups en forma periódica cada vez que el caso lo requiera y considerando también que los medios magnéticos son susceptibles y se pueden deteriorar.
iv Almacenamiento de los backups en locales diferentes donde reside la información primaria.
v Realizar pruebas periódicas de los backups, verificando su integridad.
vi La información debe salvarse por áreas usuarias, fechas y nombres de usuarios según formato.

Formación de equipos operativos de trabajo
En cada área operativa de la Municipalidad Distrital de San Sebastián, donde procesan y almacenan información técnica, útil para dicha área y la MDSS, se debe designar a un empleado responsable de la seguridad de la Información que tenga conocimientos básicos de computación e Informática, pudiendo ser el Gerente, Sub Gerente, la Secretaria u otro servidor de preferencia trabajador permanente o que, el Gerente o Sub Gerente considere conveniente, **quién** a su vez coordinará con el responsable de supervisar el cumplimiento del Plan de Contingencias, que para este caso debe ser un servidor de la Oficina de Tecnología y Sistemas Informáticos o el de turno.

Las actividades específicas que debe realizar el responsable de supervisar el Plan de Contingencias de la OTSI, serán:

- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos el Plan de Contingencias
- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos del área en cuanto a Sistemas Municipales, archivos de datos, software de fábrica Software de gestión, etc., priorizando la seguridad para los principales Sistemas y Sub Sistemas.
- Supervisar procedimientos de respaldo y restauración, vale decir, capacitar a los usuarios correspondientes y encargados de la seguridad de la información técnica de cada área.
- Supervisar la Carga de archivos de datos de las aplicaciones, y la creación de los respaldos incrementales, es decir que diariamente, que, se ingrese información a los Sistemas Municipales se realice el backup pertinente.
- En lo relacionado a la Red, las líneas de comunicaciones, entre servidores y clientes, módems, y otros aditamentos deben estar en perfectas condiciones de funcionamiento para poder establecer los procedimientos de seguridad de la información en los sitios de recuperación después de haber ocurrido el desastre.
- Organizar la prueba de hardware y software, las pruebas totales de hardware y comunicaciones son básicas e imprescindibles para prevenir el desastre, acciones que debe realizarlas el supervisor del plan de contingencias con el responsable de cada área. Lo mismo debe ocurrir con el Software.
- Ejecutar trabajos de recuperación, acciones propias que deben realizarse después del desastre.
- Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
- Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.
- Establecer y llevar a cabo procedimientos para restaurar equipos e información en lugar del desastre Participar en las pruebas y simulacros de desastres.

Formación de equipos de evaluación (auditoria de cumplimiento de los procedimientos sobre Seguridad)

Esta función será realizada por el personal técnico especializado de la Oficina de Control Interno del MDSS, caso contrario la realizará el personal técnico especializado de la Oficina de Tecnología y Sistemas Informáticos, debiendo actuar conforme y considerando claramente sus funciones, responsabilidades y objetivos.

- Revisar que las Normas y procedimientos con respecto a backups y seguridad de equipos y data se cumpla.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, su adecuado registro y almacenamiento.
- Revisar la relación entre los Sistemas Informáticos Municipales y la información técnica digitalizada, necesaria para la buena marcha de la Institución.

- Informar al comité de contingencias de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.

2.2.3.2. Actividades Durante el Desastre

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

- Plan de Emergencias
- Formación de Equipos
- Entrenamiento

Plan de emergencias

En este plan se establecen las acciones que se deben realizar cuando se presente un siniestro; así como la difusión de las mismas. Es conveniente prever los posibles escenarios de ocurrencia del siniestro, durante el día, noche o madrugada.

Este plan debe incluir la participación y actividades a realizar por todas las personas involucradas, así como las personas que podrían encontrarse presentes en el área donde ocurre el siniestro, debiendo detallar:

- Vías de entrada, salida o escape.
- Plan de Evacuación del Personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de formación de la Institución (si las circunstancias del siniestro l
-
- o posibilitan).
- Ubicación y señalización de los elementos contra el siniestro, (extinguidores contra incendios, cobertores contra inundaciones de agua, etc.).
- Secuencia de llamadas en caso de siniestro, tener a la mano elementos de iluminación (linternas), lista de teléfonos de emergencias de las diversas instituciones de la localidad, Bomberos / Ambulancia, PNP.
- Tener un directorio completo de todo el personal que labora en la Oficina de Tecnología y Sistemas Informáticos y de su personal (equipos de seguridad).

Formación de Equipos de Trabajo

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro. Si bien la premisa básica es la protección de la integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en un área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos informáticos, de acuerdo a los lineamientos o clasificación de prioridades, para salvar los equipos señalados en el plan de acción.

Entrenamiento

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos, para

minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, terrorismo, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la Gerencia otorga a la seguridad institucional.

2.2.3.3. Actividad después del Desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades especificadas en el Plan de Acción elaborado.

Evaluación de Desastre
Inmediatamente después que el siniestro ha concluido, se debe evaluar la magnitud del daño que se ha producido, por ejemplo; Que sistemas se han afectado, que equipos han quedado inoperativos, cuales se pueden recuperar, y en cuanto tiempo, etc. Adicionalmente se debe comunicar a la Institución con la cual tenemos el convenio de respaldo, para iniciar la recuperación del desastre según términos especificados en convenio.

Priorización de actividades del Plan de Acción
Toda vez que el Plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizando las actividades estratégicas y urgentes de nuestra institución. Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su ubicación temporal y asignación de funciones, en apoyo al personal de los sistemas afectados y soporte técnico.

Ejecución de Actividades
La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción.

Cada uno de estos equipos debe contar con un coordinador que deben reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato al responsable principal de del comité de contingencias.

Los trabajos de recuperación tendrán dos etapas:

a) Restauración del servicio informático, usando los recursos de la Institución y/o copias de respaldo que se encuentran en el otro local.

b) Volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente nítida y eficiente para no perjudicar el buen servicio a los contribuyentes de nuestro Sistema e imagen Institucional.

Evaluación de Resultados

Una vez concluidas las labores de recuperación de los sistemas informáticos que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tanbien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en sí, deben de salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para aminorar los riesgos y pérdida que ocasionaron el siniestro.

Retroalimentación del Plan de Acción

Con los resultados de la evaluación, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cuál hubiera sido el **costo** de no haber tenido nuestra Institución el plan de contingencias llevado a cabo.

Niveles de Prioridad de la Recuperación de Funciones

Las funciones críticas se generan principalmente en la Oficina de Tecnología y Sistemas Informáticos, Gerencia de Desarrollo Urbano, Gerencia de Infraestructura Pública, Centro de Defensa Civil y Gestión de Riesgo, Gerencia de Desarrollo Vial y Transporte, Sub Gerencia de Registro Civil, Administración, Logística, Contabilidad, Tesorería., Planificación y Presupuesto, Sub Gerencia de Secretaría General, Gerencia de Recursos Humanos, Procuraduría Pública Municipal, lo cual de producirse una catástrofe afectaría grandemente la economía de nuestra Municipalidad Provincial, originándose la necesidad de establecer prioridades en la recuperación del servicio informático.

2.3. FASE 4 – ESTRATEGIAS

Las estrategias de contingencia y continuidad de los servicios y/o negocios están diseñadas para identificar prioridades y determinar en forma razonable las soluciones a ser seleccionadas en primera instancia o los riesgos a ser encarados en primer lugar. Hay que decidir si se adoptarán las soluciones a gran escala, como las opciones de recuperación de desastres para un centro de datos.

2.3.1. Actividades Importantes

- La revisión de procesos, flujos, funciones y opciones de importancia crítica.
- La definición de las opciones de contingencia seleccionadas para cada riesgo identificado (nivel de componente, nivel de proceso de la MDSS).
- La revisión y depuración del cronograma maestro (Defensa Civil), incluyendo prioridades, fechas importantes en el calendario de eventos y dependencias cruzadas en diversos proyectos o áreas.
- La consolidación de soluciones de acuerdo a las funciones o áreas de servicios más importantes e identificar las estrategias globales.
- La identificación de los impactos de las soluciones y estrategias para ahorrar costos, como puede ser la selección de una solución para cubrir varios riesgos,

se deben de considerar varios elementos de costo: como el costo de crear la solución, el costo de implementar la solución, y el costo de mantener vigente dicha solución, debido a que la continuidad de las operaciones de la organización constituye el enfoque primordial, la estrategia de la MDSS rige el análisis de costos.

- La obtención de aprobaciones finales para el financiamiento, antes de que se apruebe la solución.
- La identificación de los beneficios es un elemento clave para asegurar que el costo del proyecto este equilibrado con los retornos reales de la organización.

2.3.2. Preparativos para la Identificación de Soluciones Preventivas

Los puntos que deben ser cubiertos por toda la red informática y usuarios en general son:

- Respaldar toda la información importante en medio magnético, ya sea en discos externos, cintas o CD-ROM, dependiendo de los recursos con que cuente cada área. Acordamos que lo que debe respaldarse es INFORMACION y no las aplicaciones.
- Generar discos de arranque para las máquinas dependiendo de su sistema operativo, ya sea Windows Server 2003, Windows XP, Windows 7, Windows 8, Windows Server 2012, libres de virus y protegidos contra escritura.
- Mantener una copia de antivirus más reciente en disco para emergencias (dependiendo del fabricante, variarán las instrucciones para generarlo).
- Guardar una copia impresa de la documentación de los sistemas e interfaces, al igual de los planes de contingencia definidos por el resto de las áreas.
- Instalar todos los Service Packs que el equipo necesite y llevar un registro de los mismos, en caso de formatear el equipo o desinstalar aplicaciones.

2.3.3. Medida de Precaución y Recomendación

En relación al Centro de Cómputo

- Es recomendable que el Centro de Cómputo no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados.
- Hasta hace algunos años la exposición de los Equipos de Cómputo a través de grandes ventanales, constituían el orgullo de la organización, considerándose necesario que estuviesen a la vista del público, siendo constantemente visitados. Esto ha cambiado de modo radical, principalmente por el riesgo de terrorismo y sabotaje, el robo, etc.
- 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 del Centro de Cómputo.
- Otra precaución que se debe tener en la construcción del Centro de Cómputo, es que no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.
- El acceso al Centro de Cómputo debe estar restringido al personal autorizado. El personal de la institución deberá tener su carnet de identificación siempre en un lugar visible.
- Se debe establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.

- Se recomienda que al momento de reclutar al personal se les debe hacer además exámenes psicológicos y médico y tener muy en cuenta sus antecedentes de trabajo, ya que un Centro de Cómputo depende en gran medida, de la integridad, estabilidad y lealtad del personal.
- 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.
- Deben establecerse controles para una efectiva disuasión y detección, a tiempo, de los intentos no autorizados de acceder a los sistemas y a los archivos de información que contienen.
- Se recomienda establecer políticas para la creación de los password y establecer periodicidad de cambios de los mismos.
- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.
- Establecer políticas de control de entrada y salida del personal, así como de los paquetes u objetos que portan.
- Las seguridades de las terminales de un sistema en red podrán ser controlados por medios de anulación del disk drive), cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos.
- Los controles de acceso, el acceso en sí y los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al centro de Cómputo, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo.
- Las cámaras fotográficas no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la Oficina de Tecnología y Sistemas Informáticos (OTSI).
- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.
- El modelo de seguridad a implementar, estará basado en el entorno y en la política y estrategias de la instalación.

Respecto a la Administración de Medios magnéticos - Almacén

- Debe ser administrado bajo la lógica de un almacén, esto implica ingreso y salida de medios magnéticos (sean USB's, cintas, USB's casetes, cartuchos, Discos removibles, Discos externos, CD's, DVD's, etc.), obviamente teniendo más cuidado con las salidas.
- El almacén de medios magnéticos, (cintas, USB's casetes, cartuchos, Discos removibles, CD's, DVD's, etc.) y de la información que contienen, se debe controlar para que siempre haya determinado grado de temperatura y de la humedad.
- Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.
- El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

Respecto a la Administración de Impresoras

- Todo listado que especialmente contenga información confidencial, debe ser destruido, así como el papel carbón de los formatos de impresión especiales.

- Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.
- Establecer controles respecto a los procesos remotos de impresión.

Niveles de Control

Existen dos tipos de activos en un Centro de Cómputo. Los equipos físicos y la información contenida en dichos equipos. Estos activos son susceptibles de robo o daño del equipo, revelación o destrucción no autorizada de la información clasificada, o interrupción del soporte a los procesos del servicio o negocio, etc. El valor de los activos a proteger, está determinado por el nivel de clasificación de la información y por el impacto en el servicio o negocio, causado por pérdida o destrucción del Equipo o información. Hay que distinguir los activos en nivel clasificado y no clasificado. Para los de nivel no clasificado, no será necesario control. Cualquier control debe basarse únicamente en el valor del equipo y servicios que ellos prestan. En cambio, tratándose de nivel clasificado, deben observarse además todas las medidas de seguridad de la información que estos equipos contengan.

MUNICIPALIDAD DISTRITAL DE SAN SEBASTIAN - CUSCO - SUB GERENCIA DE PLANEAMIENTO

2.3.4. Medios de Almacenamientos.

MUNICIPALIDAD DISTRITAL DE SAN SEBASTIAN CUSCO OTI

Recomendaciones para el Mantenimiento de los Discos Duros

El disco duro, requiere tener diversos cuidados de hardware para seguir trabajando de manera fluida y eficiente y prolongar su tiempo de vida útil. Entre las tareas más sencillas que podemos realizar para mantener el hardware del disco en buen estado, tenemos las siguientes:

- Tener un buen sistema de enfriamiento para el CPU.
- Evitar golpes y caídas.
- Evitar en lo posible, apagar y encender el equipo con mucha frecuencia. Si se requiere hacerlo, es recomendable re-iniciar el sistema.
- Una vez apagado el equipo esperar un tiempo prudencial de por lo menos 30 minutos, antes de volverlo a encender.
- Se recomienda realizar particiones a los discos duros para segmentar la información y evitar pérdidas de datos.
- Contar por lo menos con una partición primaria.
- Evitar el calor excesivo en el entorno donde se encuentre el PC.

- Comprobar y reparar archivos dañados o corruptos

  Una de las situaciones más comunes dentro del universo de Windows, es el daño o corrupción de los ficheros y los archivos que vamos guardando en el disco duro. Estos archivos pueden causar un daño leve o severo, según sea el caso, cada vez que son ejecutados por nuestro sistema. Es por esta razón, que detectar este tipo de archivos y repararlos es una tarea fundamental para mantener a nuestro disco duro funcionando a la perfección.

  Para reparar este tipo de archivos corruptos, es recomendable ejecutar aplicaciones del sistema, como, por ejemplo, el Scandisk de Windows o utilizar herramientas externas, como TuneUp Utilities, y ejecutar la función de análisis del disco.

- Mantener limpio el disco duro

Mantener el disco duro limpio de archivos repetidos, inservibles o que ya no usemos es importante, ya que evitará trabajo extra y permitirá evadir un sufrimiento o daño del disco por exceso de trabajo. Para hacerlo, podemos eliminar manualmente los programas que ya no utilicemos, ejecutar una limpieza de archivos temporales y por supuesto, mantener en óptimas condiciones el sistema, limpiando los registros y eliminando archivos basura utilizando herramientas del mismo sistema como el "Limpiador de espacio del disco".

- Desfragmentar el disco duro
  Una de las tareas más comunes dentro del mantenimiento de discos duros, es sin lugar a dudas, realizar un defragmentado o desfragmentación del disco con una frecuencia de por lo menos 30 días. De esta manera, mantendremos los archivos bien organizados y evitaremos trabajo extra del disco duro.

Recomendaciones para el Mantenimiento de Dispositivos de Almacenamiento Portátil.

A diario almacenamos documentos, imágenes y fotos, que compartimos, y guardamos. Esta información se está trasladando a la nube paulatinamente, pero la transición no ha sido tan rápida como lo esperaban los expertos.

Los usuarios todavía escogen diferentes unidades para almacenar en diferentes unidades, ya sea en un disco duro interno establecido dentro de los computadores o fuera de ellos en discos duros externos, MicroSD o memorias USB.

En el mercado existe gran variedad de dispositivos de almacenamiento de diferente tamaño, diseño y color, el problema es que estos dispositivos están expuestos a diferentes peligros que atentan contra su capacidad de almacenamiento. La empresa Toshiba compartió seis recomendaciones para minimizar los riesgos:

- Evite los golpes
  Hay que evitar por sobre cualquier recomendación someter el Disco Duro a golpes y, movimientos bruscos. Por lo general los discos que tenemos en un equipo portátil o de escritorio son mecánicos. Se debe cuidar el disco duro interno de todo computador ya que es el responsable de guardar el sistema operativo, programas y datos personales.

- Evite las altas temperaturas
  El calor excesivo también es peligroso para los componentes electrónicos internos del disco. Actualmente un portátil o la mayoría de ellos, vienen equipados con una adecuada ventilación. No obstante, el fabricante recomienda utilizar el equipo sobre una superficie lisa y plana, evitando colocar el mismo en lugares como una cama o sobre las piernas, obstruyendo las salidas de ventilación y dificultando la refrigeración.

  En un Pc de escritorio podemos observar el funcionamiento del ventilador que refrigera el equipo. Es necesario ser precavidos en que no se obstruya con prendas, papeles u objetos que pudieran caer involuntariamente sobre las ventilaciones del mismo.

- Realice de Backup
  El disco duro es un componente y como tal puede fallar, de hecho, fallan y generalmente lo hacen sin presentar ningún tipo de alerta o aviso al usuario. Es importante realizar regularmente un backup de la información en un segundo disco duro externo, o un disco externo de estado sólido.

- Haga mantenimientos regulares
  Copiar los archivos es una opción, pero también es necesario pensar en el mantenimiento preventivo, para ello habrá que realizar una desfragmentación del disco duro, que no es más que un proceso por el cual la información es guardada reduciendo o eliminando sectores vacíos y archivos temporales.

  Estos se producen al crear, eliminar o borrar archivos dejando zonas vacías o sin información. Luego del proceso, tendremos como resultado la eliminación de estas zonas, con un disco duro más rápido y que trabajará menos para encontrar la información requerida, prolongando por consiguiente la vida útil del mismo.

- Prevenir cortes de energía repentinos
  Verificar el estado de las baterías ante un posible corte de energía o utilizar un regulador de corriente ayudará a evitar cortes repentinos en el funcionamiento del portátil o computador. La velocidad de trabajo de un disco duro, (más de 5000 RPM) ante un corte de energía abrupto, la inercia del lector podría causar severos daños en el mismo, siendo este otro inconveniente para resguardar la vida útil del disco duro y su información.

- No a las limpiezas
  El disco duro no requiere de una limpieza interna, debemos evitar utilizar cualquier tipo de fluido en el mismo o en el interior de un portátil o computador de escritorio.

- Evite fuentes de magnetismo
  Es necesario prevenir la presencia de fuentes de magnetismo cerca de nuestro computador o portátil. Los electrodomésticos generan campos magnéticos, la presencia de estas fuentes de magnetismo u objetos que contienen imanes en su interior puede resultar perjudicial para nuestro computador.

  Cuando manipulamos un disco duro debemos evitar tocar con nuestras manos directamente el circuito eléctrico o los componentes del mismo, ya que podemos realizar una descarga de energía estática y dañar de forma definitiva estos circuitos. Si bien un disco duro externo ya se provee con una caja plástica para su uso y transporte, el reemplazo de un disco dañado requiere de estos cuidados.

Recomendaciones para el Mantenimiento de los Monitores
MONITOR CRT

- **LIMPIEZA INTERNA**
  - Hay que desconectar de la corriente y desenchufarla de la computadora, para evitar una descarga eléctrica.

- Una vez ya desconectado, hay que esperar 10 a 15 min., de manera que sus partes internas descarguen su energía. o Colocamos el monitor de lado y quitamos la base ejerciendo una suave presión sobre la solapa plástica que la traba.
- ahora ponemos una tela o trapo sobre la mesa para poder colocar la pantalla del monitor sobre esta, y así poder evitar rayones en la pantalla.
- Enseguida podremos destapar la carcasa, con un destornillador de cruz. Una vez hecho esto se va retirando la carcasa cuidadosamente, para no dañar sus cables de conexión y de video. o Una vez ya destapada la carcasa entonces lo que hay que hacer es limpiar las partes internas del monitor. La manera más recomendable es con una compresora.
- Entonces con el soplete de la compresora vamos limpiando nada más sus circuitos sin ejercer demasiada presión y sin acercar tanto el soplete porque puede que se rompa alguno de sus circuitos. o Lo más delicado de esto es su osciloscopio. Este no hay que tocarlo, si tiene tierra hay que quitársela delicadamente con una brocha no haciendo demasiada presión sobre este ya que son muy delicados.

- **LIMPIEZA EXTERNA**

- Continuamos ensamblando la carcasa al monitor y luego la base a la carcasa y monitor.
- Una vez ya unidos seguimos con "La limpieza física del monitor".
- Lo primero que hay que hacer es limpiar la carcasa y la orilla del monitor con otro paño de algodón limpio adhiriendo a este un poco de espuma de limpieza.
- Una recomendación podemos empezar de abajo hacia arriba en forma de círculos y suavemente para no introducir algo de espuma en la ventilación del monitor.
- Al finalizar seguimos con la pantalla. En esta parte nosotros no debemos humedecer otro paño con agua (para evitar rayones), sino que debe ser con alcohol isopropílico.
- Así que en forma de las manecillas del reloj limpiamos suavemente la pantalla tratando de no hacer mucha presionen ella.
- Una vez terminado esto tu monitor ya está limpio y listo para conectarse.

MONITOR LCD

Siempre recuerden que la "L" en LCD significa "líquido", recuerden que la pantalla de su monitor LCD no es tan firme como la de un monitor CRT; es plástico suave, así que tienen que tratarla con delicadeza.

Para limpiar un monitor LCD: evite cualquier cosa que contenga lejía o amoníaco, estos provocan una reacción del plástico y solo lograrían que la pantalla se opaque y pierda su color. Cualquier cosa puntiaguda, afilada o abrasiva. Olviden el detergente, alcohol, lija, o papel periódico para sacar brillo (no es vidrio).

No lanzar el spray del líquido directamente sobre la pantalla, si no disponemos de un atomizador, solo usemos una botella y coloquemos un poco de líquido

sobre el paño teniendo cuidado de no empaparlo mucho, solo humedecerlo, y haciendo esto lo más lejos posible de la pantalla.

Limpiemos la superficie de la pantalla muy suavemente con movimientos horizontales y verticales, en las zonas con manchas rebeldes, hagamos movimientos circulares lentos pero firmes.

- **LIMPIEZA INTERNA**
  - Desconectamos de la corriente y del gabinete la pantalla y esperamos 5 o 10 minutos para que descargue la energía eléctrica de sus componentes internos.
  - Ahora debe colocar el monitor sobre una tela o paño de algodón para poder destornillar su carcasa y así poder limpiar su parte interna con una compresora o aerosol limpia contactos tomando en cuenta que no hay que acercarnos tanto a los componentes para así no dañar alguno.

- **LIMPIEZA EXTERNA**
  - Una vez terminado, cerramos la carcasa y seguimos limpiando, pero ahora su carcasa de manera física. o Se recomienda empezar por su carcasa y al último su pantalla, así que colocamos la pantalla sobre una tela o paño de algodón para evitar rayones.
  - Para limpiar la carcasa y el contorno de la pantalla nosotros debemos obtener un paño de algodón limpio, adhiriendo espuma de limpieza y de limpiar de manera suave sin ejercer demasiada presión
  - Una vez terminado esto, levantas el monitor y continuamos la limpieza con la pantalla.

Recomendación para el Cuidado del Equipo de Cómputo

- Generar una copia de seguridad de tu información, mínimo una vez al mes (de preferencia emplea un disco duro externo).

- Usar un buen sistema de protección eléctrica, preferible usa un buen UPS (Unit Power Supply = Sistema de Alimentación Ininterrumpida).

- Realizar mantenimiento preventivo a tu pc o laptop mínimo una vez al año.

- No tapes los orificios de ventilación de tu equipo de cómputo, ni lo encierres totalmente. El calor es su peor enemigo.

- Tener un buen antivirus debidamente actualizado, mejor si incluye firewall, antispyware, antimalware, y antiroot kits.

- Recuerda, has una copia de seguridad de tu información, mínimo una vez al mes.

- Rechaza archivos que te lleguen por email, MSN, de procedencia dudosa o que no hallas solicitado, es la principal forma de trasmisión de virus y otras amenazas.

- No brinde a extraños ni deje que su máquina recuerde sus claves tanto de información virtual como física (emails, chats, números de tarjetas de crédito, etc).

- La empresa o persona que haga el mantenimiento de su pc que sean de una reputación intachable, ellos tendrán acceso a TODA nuestra información.

Mantener las Áreas Operativas Limpias y Pulcras

La MDSS cuenta con muchas razones para mantener las áreas operativas limpias y pulcras, sin embargo, es imposible lograr este objetivo en su totalidad, algunos de los problemas o peligros que se pueden evitar son:

- El daño potencial al equipo por derramar el café, leche o chocolate u otros líquidos en los componentes de los equipos computarizados,
- El peligro de fuego que se presenta por el excesivo almacenamiento de hojas continuas,
- El peligro por fumar en los ambientes informáticos y las falsas alarmas creadas por detectores de humo.
- Deficientes instalaciones eléctricas que generan contantes cortocircuitos.
- Deficiente cableado de redes que contribuyen a la perdida de información.
- Acumulación de materiales inflamables y no inflamables en diferentes áreas municipales.

Estos son solamente algunos de los problemas encontrados en las áreas operativas con reglas poco estrictas de limpieza, sobretodo de orden.

2.4. FASE 5 - DOCUMENTACION DEL PROCESO

Todo el proceso de lograr identificar soluciones ante determinados problemas no tendrá su efecto verdadero si es que no se realiza una difusión adecuada de todos los puntos importantes que este implica, y un plan de contingencia con mucha mayor razón necesita de la elaboración de una documentación que sea eficientemente orientada.

Como puntos importantes que debe de incluir esta documentación podremos citar las siguientes:

1. Plan de trabajo para organizar las actividades del Plan de Contingencias.
2. Cuadro de descripción de los equipos y las tareas para ubicar las soluciones a las contingencias.
3. La documentación de los riesgos, opciones y soluciones por escrito y en detalle.
4. La identificación y documentación de listas de contacto de emergencia, la identificación de responsables de las funciones con el fin de garantizar que siempre haya alguien a cargo, y que pueda ser contactada si falla un proceso de importancia.

2.5. FASE 6 - REALIZACION DE PRUEBAS Y VALIDACION

2.5.1. Plan de Recuperación de Desastres

- Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en la Oficina de Tecnología y Sistemas Informáticos, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora.
- Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

- La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, deben ser planeados y probados fehacientemente.
- Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Institución.
- Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.
- Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:
  - Actividades Previas al Desastre.
  - Actividades Durante el Desastre.
  - Actividades Después del Desastre

Actividades Previas al Desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de recuperación con el menor costo posible a nuestra institución.

Podemos detallar las siguientes Actividades Generales:

i. Establecimiento del Plan de Acción.
ii. Formación de Equipos Operativos.
iii. Formación de Equipos de Evaluación (auditoría de cumplimiento de los procedimientos sobre Seguridad).

i Establecimiento del Plan de Acción

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a:

a) Sistemas e Información. - la Institución deberá tener una relación de los Sistemas Informáticos con los que cuenta, tanto los realizados por la Oficina de Tecnología y Sistemas Informáticos, como los del Estado, así como los desarrollados por terceros y/o dados en uso con otras instituciones, debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional.

La relación de sistemas informáticos deberá detallar los siguientes datos:

- Nombre del sistema.
- Lenguaje o paquete con el que fue creado el sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).
- La Unidad Orgánica (Gerencia, Sub Gerencia, Centro, etc.) que genera la información base (el «dueño» del sistema).
- Las Unidades funcionales (departamentos, oficinas, áreas, etc.) que usan la información del sistema.
- El volumen de los archivos que trabaja el sistema.
- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema
- El equipamiento necesario para un manejo óptimo del sistema.

- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este sistema para la institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema).
- Equipamiento mínimo necesario para que el sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
- Actividades a realizar para volver a contar con el sistema informático (actividades de restore).

Con toda esta información se deberá de realizar una lista priorizada (un ranking) de los sistemas informáticos necesarios para que la Institución pueda recuperar su operatividad perdida en el desastre (contingencia).

b) **Equipos de Cómputo**. - aparte de las Normas de Seguridad que se verán en los capítulos siguientes, hay que tener en cuenta:

- Inventario actualizado de los equipos de manejo de información (computadoras, lectoras de microfichas, impresoras, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional.
- Pólizas de Seguros Comerciales. Como parte de la protección de los activos institucionales, pero haciendo la salvedad en el contrato, que, en casos de siniestros, la restitución del computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.
- Señalización o etiquetado de los computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo, etiquetar (colocar un sticker) de color rojo a los servidores, color amarillo a las PC's con Información importante o estratégica y color verde a las PC's de contenidos normales.
- Tener siempre actualizada una relación de PC's requeridas como mínimo para cada sistema permanente de la Institución (que por sus funciones constituyen el eje central de los servicios informáticos de la Institución), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos sistemas.

c) **Obtención y Almacenamiento de los Respaldos de Información (BACKUPS)**. - se deberá establecer los procedimientos para la obtención de copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

- Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).
- Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).

- Backups del Software Aplicativo (considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.
- Backups de los Datos (Bases de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).
- Backups del Hardware. Se puede implementar bajo dos modalidades:

Modalidad Externa. Mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.

Modalidad Interna. Si tenemos más de un local, en ambos debemos tener señalados los equipos, que, por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos.

En ambos casos se deberá probar y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

d) **Políticas (Normas y Procedimientos de Backups)**. - Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente en el punto «c», debiéndose incluir:

- Periodicidad de cada Tipo de Backup.
- Respaldo de Información de movimiento entre los períodos que no se generan Backups (backups incrementales).
- Uso obligatorio de un formulario estándar para el registro y control de los Backups.
- Correspondencia entre la relación de sistemas e información necesaria para la buena marcha de la empresa, y los backups efectuados.
- Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).

- Almacenamiento de los Backups en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local estudiado).
- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

ii. Formación de Equipos Operativos

En cada unidad operativa de la institución, que almacene información y sirva para la operatividad institucional, se deberá designar un Responsable de la Seguridad de la Información – RSI de su unidad. Pudiendo ser el jefe de dicha Área Operativa. Sus labores serán:

- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
- Supervisar procedimientos de respaldo y restauración.
- Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos incrementales.
- Coordinar líneas, terminales, módem, otros aditamentos para comunicaciones.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software.
- Ejecutar trabajos de recuperación.
- Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
- Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.
- Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- Participar en las pruebas y simulacros de desastres.

iii. Formación de Equipos de Evaluación (Auditoría de cumplimiento de los procedimientos sobre seguridad)

Esta función debe ser realizada de preferencia por personal externo con experiencia en Seguridad de la Información, de no ser posible, la realizará el personal de la Oficina de Tecnología y Sistemas Informáticos, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

- Revisar el cumplimiento de las normas y procedimientos con respecto a Backups y seguridad de equipos y data.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Revisar la correlación entre la relación de sistemas e informaciones necesarios para la buena marcha de la institución, y los backups realizados.

- Informar de los cumplimientos e incumplimientos de las normas, para las acciones de corrección respectivas.

Actividades Durante el Desastre

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

i. Plan de Emergencias.
ii. Formación de Equipos.
iii. Entrenamiento.

i. Plan de Emergencias

En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas. Es conveniente prever los posibles escenarios de ocurrencia del Siniestro:

- Durante el día.
- Durante la noche o madrugada.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

- Vías de salida o escape.
- Plan de Evacuación del Personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan)
- Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Policía Nacional del Perú y de su personal (equipos de seguridad) asignados para estos casos.

ii. Formación de Equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro. Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en un área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

iii. Entrenamiento.

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden

realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

Actividad Después del Desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción.

i Evaluación de Daños.
ii Priorización de Actividades del Plan de Acción
iii Ejecución de Actividades
iv Evaluación de Resultados
v Retroalimentación del Plan de Acción.

i. Evaluación de Daños

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se deberá lanzar un pre-aviso a la Institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha Institución.

ii. Priorización de Actividades del Plan de Acción

Toda vez que el Plan de Acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

iii. Ejecución de Actividades

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del sistema de información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro sistema e imagen institucional,

como para no perjudicar la operatividad de la institución o local de respaldo.

iv. Evaluación de Resultados

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en sí, deberían de salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

v. Retroalimentación del Plan de Acción

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cuál hubiera sido el costo de no haber tenido nuestra institución el plan de contingencias llevado a cabo.

2.6. FASE 7 - IMPLEMENTACION

La fase de implementación se da cuando han ocurrido o están por ocurrir los problemas para este caso se tiene que tener preparado los planes de contingencia para poder aplicarlos. Puede también tratarse esta etapa como una prueba controlada.

2.6.1. De las Emergencia Físicas

CASO A: Error Físico de Disco de un Servidor (Sin RAID)

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

- Ubicar el disco malogrado.
- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
- Bajar el sistema y apagar el equipo.
- Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
- Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
- Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
- Habilitar las entradas al sistema para los usuarios.

CASO B: Error de Memoria RAM

En este caso se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.
- Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto, si hubiese un error de paridad, el servidor se autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la OTSI, a menos que la dificultad apremie, cambiarlo inmediatamente. Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Ubicar las memorias malogradas.
- Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
- Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
- Probar los sistemas que están en red en diferentes estaciones.
- Finalmente, luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO C: Error de Tarjeta(s) Controladora(s) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Ubicar la posición de la tarjeta controladora.
- Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
- Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
- Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

CASO D: Caso de Incendio Total

En el momento que se dé aviso por los altavoces de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos en cintas magnéticas.

- Ante todo, se recomienda conservar la serenidad. Es obvio que, en una situación de este tipo, impera el desorden, sin embargo, es muy recomendable

tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es).
- Se apagará (poner en OFF) la caja principal de corriente de la Oficina de Tecnología y Sistemas Informáticos.
- Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

CASO E: Caso de Inundación

- Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.
- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
- Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.
- Para prevenir los cortos circuitos, asegurarse de que no existan fuentes de líquidos cerca de las conexiones eléctricas.
- Proveer cubiertas protectoras para cuando el equipo esté apagado.

CASO F: Caso de Fallas de Fluido Eléctrico

Se puede presentar lo siguiente:

- Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.
- Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia[1]), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.
- Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (o UPS).

Se contará con transformadores de aislamiento (nivelan la corriente) asegurando que la corriente que entre y salga sea 220v, evitando que los equipos sufran corto circuito por elevación de voltaje (protegiendo de esta manera las tarjetas, pantallas y CPU del computador).

2.6.2. De las Emergencias Lógicas de Datos

CASO A: Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.

- Fallas causadas usualmente por un error de chequeo de inconsistencia física

En caso de producirse alguna de las situaciones descritas anteriormente; se debe realizar las siguientes acciones:

PASO 1: verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos, una vez mostrado el prompt de DOS, cargar el sistema operativo de red.

PASO 2: deshabilitar el ingreso de usuarios al sistema.

PASO 3: descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.

PASO 4: cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

PASO 5: al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente. Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

CASO B: Caso de Virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

- Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Estos archivos (exe, com, ovl, nlm, etc.) serán reemplazados del diskett y/o CD original de instalación o del backup.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

Se revisará las computadoras que no estén en red con antivirus de USB's. De suceder que una computadora se haya infectado con uno o varios virus ya sea en la memoria o a nivel disco duro, se debe proceder a realizar los siguientes pasos:

- Utilizar un USB's que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado.
- Reiniciar el computador con dicho USB's.
- Retirar el USB's con el que arrancó el computador e insertar el USB's antivirus, luego activar el programa de tal forma que revise todos los archivos y no sólo los ejecutables.
- De encontrar virus, dar la opción de eliminar el virus.
- Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren, si éstos son varios pertenecientes al mismo programa, reinstalar al término del Escaneado.
- Finalizado el escaneado, reconstruir el Master Boot del disco duro

2.7. FASE 8 – MONITOREO

La fase de Monitoreo nos dará la seguridad de que podamos reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da un cambio en la infraestructura, debemos de realizar un mantenimiento correctivo o de adaptación.

Un punto donde se tiene que actuar es por ejemplo cuando se ha identificado un nuevo riesgo o una nueva solución. En este caso, toda la evaluación del riesgo se cambia, y comienza un nuevo ciclo completo, a pesar de que este esfuerzo podría ser menos exigente que el primero.

Esto es importante ya que nos alimentamos de las nuevas posibilidades de soluciones ante nuevos casos que se puedan presentar, podríamos enumerar las actividades principales a realizar:

1. Desarrollo de un mapa de funciones y factores de riesgo.
2. Establecer los procedimientos de mantenimiento para la documentación y la rendición de informes referentes a los riesgos.
3. Revisión continúa de las aplicaciones.
4. Revisión continua del sistema de backup
5. Revisión de los Sistemas de soporte eléctrico del Centro de Procesamiento de Datos.

CONCLUSIONES

- La Municipalidad Distrital de San Sebastián, es una institución de servicio muy importante por lo que es necesario que cuente con un Plan de Contingencias de Sistemas de Información bien estructurado y que sea posible su implementación.
- El Plan de Contingencias de Sistemas de Información elaborado por la Oficina de Tecnología y Sistemas Informáticos de la MDSS, debe ser evidenciado oportunamente a fin de que su aplicación sea fácil en el momento preciso.
- El mencionado plan debe contar con el presupuesto necesario a fin de cubrir la capacidad de la infraestructura física, así como las funciones que realiza La Oficina de Tecnología y Sistemas Informáticos de la MDSS.
- El Plan de Contingencias de Sistemas de Información es un documento de gestión y debe ser considerado en los Plan Operativo Institucional, Plan Operativo Informático y desde luego en los Cuadros de Necesidad en cada periodo.

RECOMENDACIONES

- El presente Plan de Contingencias debe ser aprobado por Resolución de Alcaldía con la finalidad de poder realizar las pruebas y aplicaciones correspondientes.
- Se recomienda activar el comité de sistemas aprobado con R.A. 027-94. para que dicho comité participe activamente en el Plan de Contingencias Informático.
- Organizar el Plan de trabajo e involucrar al personal correspondiente y dar inicio a las labores del Plan de Contingencias.
- Solicitar el presupuesto necesario, para poder desarrollar el Plan de Contingencias.
- Informar oportunamente a la Alcaldía y a la Gerencia Municipal con el fin de recibir el apoyo político y administrativo necesario.

GLOSARIO

Acceso
Es la autorización para ingresar y recuperar o grabar datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

Acceso no autorizado a la información
Si no existen medidas de seguridad se pueden producir accesos no autorizados a los sistemas, computadoras personales, terminales de red e información confidencial.

Amenaza
Cualquier cosa que pueda interferir el funcionamiento adecuado de una computadora personal o Servidor de Bases de Datos, o causar la difusión no autorizada de información confiada a una computadora, Ejemplo, fallas del suministro eléctrico, virus, saboteadores o usuarios descuidados.

Análisis de Riegos
Evaluación económica del impacto de estos sucesos negativos valor que servirá para contrastar el costo de protección de la información versus el costo de volverla a reproducir.

Ataque
Termino General usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

Ataque Activo
Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora o hace que se difunda de modo no autorizado información confiada a una computadora personal o Servidor de Bases de Datos: ejemplo el borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el buen funcionamiento de una computadora.

Ataque Pasivo
Intento de obtener información o recursos de una computadora sin interferir con su funcionamiento, ejemplo, espionaje electrónico o la intercepción de una red. Todo esto puede dar información importante sobre el Sistema, así como permitir la aproximación de los datos que contiene.

Base de Datos
Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que, además, están almacenados con criterios independientes de los programas que los utilizan. También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System-DBMS).

Las características que presenta un DBMS son las siguientes:
Brinda seguridad e integridad a los datos.
Provee lenguajes de consulta (interactivo).
Provee una manera de introducir y editar datos en forma interactiva.

Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

Contingencia
Cualidades o características necesarias de lo contingente, es decir de lo que puede suceder o no suceder.

Datos
Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.
En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

Emergencias físicas
Error físico de disco de un servidor memoria, tarjetas, fluido eléctrico, inundaciones, incendio, etc.

Emergencias lógicas
Error lógico de datos, virus etc.

Incidente
Cuando se produce un ataque o se materializa una amenaza, ejemplo, intento de borrar archivos o fallas del fluido eléctrico

Golpe
Impacto producido por una persona intencionalmente o no intencionalmente, a un equipo informático el cual será perjudicial en su funcionamiento.

Integridad
Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.
El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

Plan de contingencias
Un Plan de contingencias es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño, dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía. Un plan de contingencias es un caso particular de plan de continuidad aplicado al departamento de informática o tecnologías.

Plan de recuperación de desastres
La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia debe ser planeada y probados fehacientemente previa autorización de la máxima autoridad de turno.

Privacidad
Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

Protección especial de la información
Métodos especiales para proteger la información mediante técnicas criptográficas.

Seguridad
Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.