MUNICIPALIDAD PROVINCIAL

DE BARRANCA

Plan de Contingencia Informático de la Municipalidad Provincial de Barranca

PRESENTACION

Uno de los más importantes activos de toda institución es la información que ésta genera en sus diferentes acciones y ámbitos. Conscientes de esta premisa, podemos indicar que se debe adoptar medidas de seguridad para la información y así mismo estar preparados para poder afrontar contingencias y desastres de tipo adverso.

La Unidad de Estadística y Sistemas, tiene entre otros, el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones institucionales. En base a ello presenta el Plan de Contingencia Informático de la Municipalidad Provincial de Barranca.

En la actualidad, los profesionales y técnicos de la informática tienen como una de sus principales actividades y preocupaciones la seguridad de estos sistemas, que constituyen una base y respaldo a las funciones institucionales realizadas a través de los años, así como en la actualidad facilitan a sobre manera las tareas que se desarrollan en la ejecución de los diferentes procesos administrativos, logísticos, ejecutivos, informativos, sociales de planeamiento y de servicios.

Los responsables del servicio informático están obligados a hacer de conocimiento y explicar con lenguaje entendible a estos directivos las posibles consecuencias que la inseguridad insuficiente o inexistente pueda acarrear, de esa manera proponer y poner a consideración las medidas de seguridad inmediatas y a mediano plazo, que han de tomarse para prevenir los desastres que pueda provocar el colapso de los sistemas.

GENERALIDADES

A. OBJETIVO

Formular un adecuado Plan de Contingencias, que permita la continuidad en los procedimientos informáticos de la Unidad de Estadística y Sistemas, así como enfrentarnos a 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; buscando la mejora de la calidad en los servicios que brinda la Unidad de Estadística y Sistemas.

B. BASE LEGAL

1. D.L. 604. Ley de Organización y Funciones del INEI
2. Resolución Jefatural N°018-91-INEI, Norma Técnica para el procedimiento y respaldo de la información que se procesa en entidades del Estado.
3. Resolución Jefatural N° 340-94-INEI, que aprueba la Directiva "Normas Técnicas para el Almacenamiento y Respaldo de la Información que se procesa en las Entidades del Estado".
4. Resolución Jefatural N° 076-95-INEI Recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.
5. Resolución Jefatural N° 090-95INEI Recomendaciones Técnicas para la protección física de los equipos y medios de procesamientos de la información en la administración pública.
6. Ley Orgánica de Municipalidades N°27972 Art 20° inciso 6) del 27-05-2003 (dictar decretos y resoluciones de alcaldía, con sujeción a las leyes y ordenanzas)
7. Decreto Supremo N° 033-2018-PCM, se crea la Plataforma Digital Única del Estado Peruano.
8. Resolución Ministerial N°119-2018-PCM se dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.
9. Resolución Ministerial N°004-2016-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.
10. Resolución Ministerial N° 119-2018-PCM, se dispone la creación del Comité de Gobierno Digital en cada entidad de la Administración Pública.
11. Decreto Supremo N°033-2018-PCM se crea la Plataforma Digital Única del Estado Peruano.

C. ALCANCE

El Plan de Contingencias Informático está basado en la realidad que manifiesta la Municipalidad Provincial de Barranca (MPB) y puede servir como punto de partida hacia la adecuación y establecimiento de políticas tanto en la Municipalidad como en las diferentes oficinas. Un plan de Contingencias debe ser diseñado y elaborado de acuerdo con la necesidad y realidad de cada institución, tener sus propios requerimientos, tener que adoptar un sitio especial para el procesamiento de la información o hasta tener que construirlo o implementarlo, requerirá además de pruebas de procedimientos nuevos y que sean compatibles con los procesos existentes, incluso muchas veces se requerirá

contar con la participación de personal de otras oficinas o áreas para trabajar en conjunto cuando se desarrollen o implementen soluciones.

D. META

Potenciar el nivel informático de la Unidad de Estadística y Sistemas de la MPB, y además las funciones cotidianas informáticas, haciéndolas seguras y consistentes, logrando con ello su buen desarrollo y la optimización de resultados.

CAPITULO I

SITUACION ACTUAL

A. DIAGNOSTICO

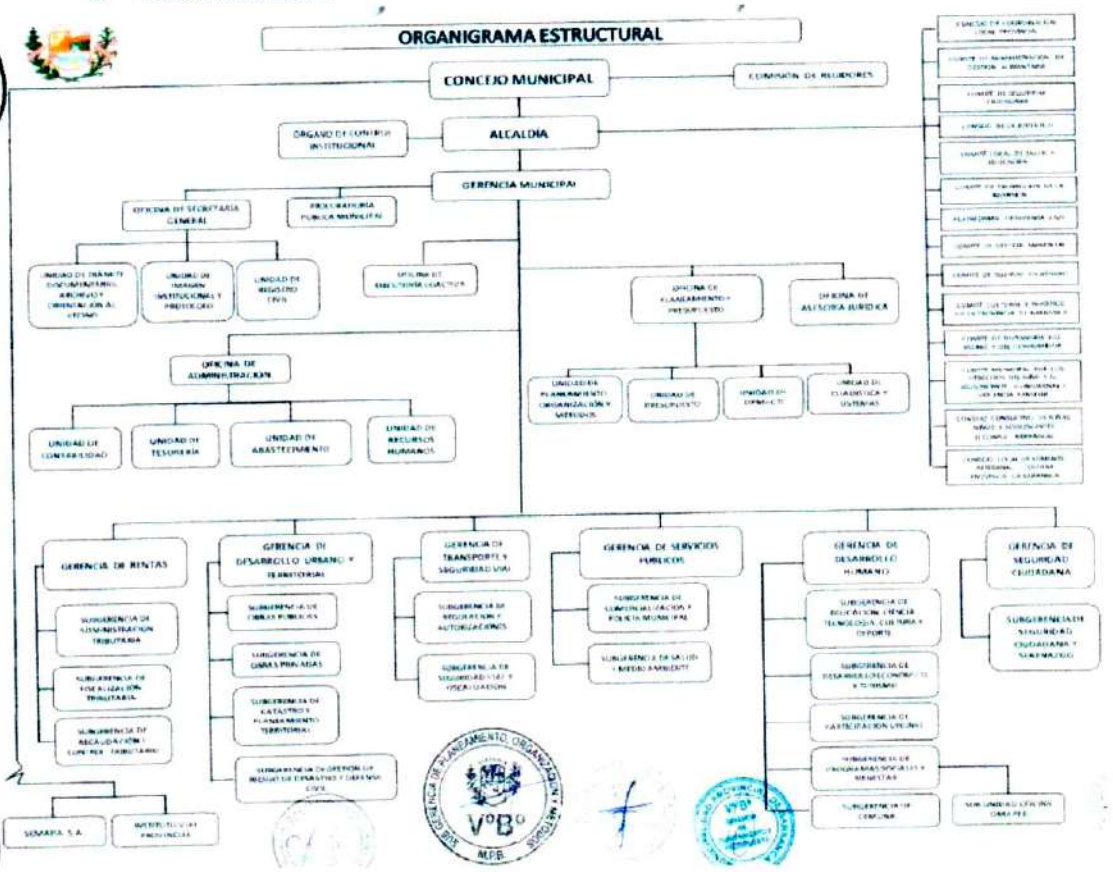
Efectuada nuestra revisión de la administración de riesgos de tecnologías de información de la Municipalidad Provincial de Barranca consideramos que debe desarrollarse un Plan de Contingencias. Si bien hemos observado la existencia de normas, procedimientos y controles que cubren algunos aspectos de 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 se ha verificado 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, estos controles 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.

B. ORGANIZACIÓN

1. ORGANIGRAMA



2. ESTRUCTURA Y FUNCIONES

a. **Alcaldía.** Es el órgano de alta dirección y a la vez el Órgano Resolutivo de la Municipalidad Provincial de Barranca. El Alcalde es el representante legal de la Municipalidad, ostenta la condición de Funcionario Público (FP), y la máxima autoridad administrativa.

b. **Gerencia Municipal.** Es el órgano de alta dirección encargado de la administración municipal. Le corresponde conducir y articular el planeamiento, organización, ejecución, evaluación y supervisión de las actividades que realiza la Municipalidad dentro del marco de los lineamientos de política establecidos por el Concejo Municipal Provincial, el alcalde y las disposiciones legales y normativas vigentes.

c. **Procuraduría Pública Municipal.** Es parte del Sistema Administrativo de Defensa Jurídica del Estado. Se encuentra vinculada administrativamente y funcionalmente a la Procuraduría General del Estado y se rige por la normativa vigente en la materia.

d. **Ejecutoría Coactiva.** Es el órgano de control encargado de planificar, ejecutar, controlar y mejorar los procedimientos de ejecución coactiva de obligaciones de naturaleza tributaria y no tributaria, garantizando a los obligados el derecho a un debido procedimiento coactivo al amparo de la Ley N°26979.

e. **Oficina de Asesoría Jurídica.** Encargada de ejecutar funciones consultivas en materia jurídica, así como brindar asesoramiento sobre la adecuada interpretación, aplicación y difusión de las normas legales y de competencia municipal, principalmente emite informes y opiniones de carácter jurídico para un pronunciamiento adecuado e imparcial para los interesados internos o externos por parte de la Municipalidad.

f. **Oficina de Planeamiento y Presupuesto.** Encargada de los sistemas administrativos de Planificación estratégica, Presupuesto Público, Inversión Pública, Modernización del Estado y Endeudamiento Público. Asimismo, le corresponde asumir la supervisión de la gestión y la dirección de la estadística, sistemas informáticos y Cooperación Técnica Internacional.

g. **Oficina de Secretaria General.** Encargada de brindar soporte administrativo al Concejo Municipal y la Alcaldía, es responsable de coordinar la conducción de los procesos de Trámite Documentario, Archivo y Orientación al Vecino, Imagen Institucional y Protocolo y Registro Civil.

h. **Oficina de Administración.** Encargada de la administración de los recursos humanos, económicos y financieros asignados a la entidad. Tiene bajo su ámbito la administración de las actividades derivadas de los sistemas administrativos en materia de Gestión de Recursos Humanos, Abastecimiento, Contabilidad y Tesorería de la Municipalidad Provincial de Barranca.

i. **Gerencia de Rentas.** Encargada de planificar, ejecutar, controlar las actividades de registro, recaudación y administración de los ingresos tributarios y no tributarios de la Municipalidad Provincial de Barranca conforme a la legislación sobre la materia.

j. **Gerencia de Desarrollo Urbano y Territorial.** Encargada de conducir los procesos de planeamiento y control de la infraestructura urbana y rural, administración del catastro, ejecución y control de las obras públicas y privadas, supervisión de edificaciones y habitaciones urbanas, supervisión de la ejecución del Planeamiento Territorial, basado en el Ordenamiento Territorial y la Zonificación Ecológica y Económico de la Provincia y el área técnica municipal (ATM), así como la supervisión de la emisión de autorizaciones, certificaciones, concesiones y adjudicaciones en el marco de la legislación vigente sobre la materia.

k. **Gerencia de Transporte y Seguridad Vial**. Encargada de planificar, conducir y supervisar la ejecución de los procesos de regulación y autorizaciones del tránsito y transporte regular y no regular, así como de la seguridad vial y la fiscalización sobre el cumplimiento de las regulaciones en el ámbito de la Provincia de Barranca y en el marco de la legislación vigente.

l. **Gerencia de Servicios Públicos.** Encargada de formular, proponer, supervisar y cumplir las políticas de servicios públicos, adecuadas al ordenamiento territorial y zonificación ecológica y económica, en especial al Sistema Local de Gestión Ambiental SLGA, así como, de planificar, ejecutar, controlar y mejorar la gestión de los procesos a cargo de las subgerencias bajo su mando, en el marco de la legislación vigente.

m. **Gerencia de Desarrollo Humano.** Encargado de promover, gestionar y participar activamente en la generación de alianzas estratégicas y mecanismos de cooperación con entidades públicas y privadas, y organismos internacionales especializadas en ciencia, tecnología e innovación tecnológica con la finalidad de desarrollar y poner en valor los diseños, inventarios y adaptaciones tecnológicas a nivel piloto, desarrollados por los estudiantes de educación regular, educación superior no universitaria o educación universitaria, así como para impulsar proyectos científicos realizados por los institutos públicos de investigación, centros de investigación públicos y privados y organismos internacionales que promuevan el desarrollo de la ciencia, tecnología e innovación y salud; promover el bienestar social; facilitar, articular y fortalecer espacios de participación de la ciudadanía, promover el mejoramiento de las condiciones de vida de la población más vulnerable; la reinserción social de los niños y jóvenes en riesgo, de personas con discapacidad, de adultos mayores, mujeres y familias en situación de pobreza y extrema pobreza, y de la promoción del turismo, de desarrollo empresarial, comercial, industrial y servicios profesionales, dentro del marco de las disposiciones legales vigentes en la materia. Los programas sociales y bienestar, comprenden: Programa de Vaso de Leche (PVL); Programas de complementación alimentaria (PCA y PANTBC) Sistema de focalización de hogares (SISFOH), así como la DEMUNA,

OMAPED, ADULTO MAYOR y otros que interrelacionan el bienestar de la comunidad.

n. **Gerencia de Seguridad Ciudadana.** Encargada de cautelar el cumplimiento de la legislación de competencia municipal y proporcionar condiciones adecuadas de seguridad ciudadana al vecino, a través de acciones de prevención contra situaciones de violencia o delincuencia; se encarga de contribuir a mantener el orden y el respeto de las garantías individuales, sociales y bienestar social dentro de la jurisdicción de la Provincia, en coordinación con la Policía Nacional del Perú.

C. RECURSOS INSTITUCIONALES

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

1. Humanos

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 Unidad de Estadística y Sistemas 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 ser denominador común para su aplicación. Por último las personas de diferentes áreas de la Municipalidad Provincial de Barranca que servirán de nexo para la captura de información y definición de tareas del plan.

2. Materiales

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

3. Financieros

Los recursos financieros con que se requiere contar para la aplicación del presente Plan de Contingencia, serán indicados en el Plan Operativo Informático 2024.

4. Entrenamientos

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.

5. Responsabilidad

La alta dirección 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.

D. SERVICIOS Y/O BIENES PRODUCIDOS

La Municipalidad Provincial de Barranca es una institución que se encarga de brindar servicios a los vecinos de Barranca como:

1. Promover la participación vecinal
2. Fortalecer la seguridad ciudadana
3. Mantener los parques y jardines
4. Garantizar el control sanitario
5. Conservar el medio ambiente
6. Promover el bienestar social
7. Fomentar la cultura, el deporte y el turismo
8. Proveer limpieza pública
9. Mantener la infraestructura vial
10. Administrar el Registro Civil

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

E. INVENTARIO DE RECURSOS INFORMÁTICOS

1. COMPUTADORAS

El inventario actual será mostrado en el Anexo 01

2. SOFTWARE UTILIZADO

El software utilizado en la Municipalidad Provincial de Barranca se muestra en el siguiente cuadro:

Sistemas Operativos		Lenguajes de Programación	
	Microsoft Windows Server 2016		Visual Studio .NET
	Linux Red Hat		
	Microsoft Windows 10	Suite de Oficina	
	Microsoft Windows 7		Microsoft Office
Base de Datos		Sistemas Antivirus	
	Sql Server 2012		ESET Nod32
	PostgreSQL		

3. APLICATIVOS INFORMATICOS

Sistema	Nombre del Sistema	Descripción	Responsable Funcional
SIGEM	Sistema de Gestión Municipal	Administra los procesos administrativos y tributarios de la Municipalidad. Se encuentran los módulos administrativos: Rentas, Registro Civil, Administración Tributaria. Predial, Fraccionamiento, Coactivo, Caja	Gerencia de Rentas, Unidad de Registro Civil, Administración Tributaria, Tesorería
Registro Civil	Sistema de Registro Civil	Inscribe las partidas civiles de nacimiento, matrimonio y	Unidad de Registro Civil

		defunción de los recurrentes y no recurrentes del distrito.	
Tramite Documentario	Sistema de Tramite Documentario	Permite la creación de expedientes presentados por los ciudadanos, los mismos que son enviadas a áreas determinadas según los asuntos	Todas las áreas
SIAF	Sistema de Integración de Administración Financiera	El SIAF es un sistema que automatiza los procedimientos financieros para registrar los recursos públicos recaudados y aplicarlos a la concreción de los objetivos del sector público. Los módulos con los que	Unidad de Presupuesto, Abastecimiento, Contabilidad, Administración, Recursos Humanos
SIGA	Sistema Integrado de Gestión Administrativa	Es una herramienta informática que simplifica y automatiza los procesos administrativos en una entidad del Estado	Todas las áreas
SGD	Sistema de Gestión Documental	Controla de modo eficiente y sistemático, la creación, la recepción, el mantenimiento, la utilización y la disposición de los documentos	Todas las áreas (Actualmente inoperativo)
Portal Web	Portal Web	Publicación de la información general de la Municipalidad	Secretaria General, Obras Públicas, Imagen Institucional, Contabilidad, Recursos Humanos, Planeamiento y Presupuesto, Administración, Abastecimiento

CAPITULO II

FASE DE REDUCCIÓN DE RIESGOS

A. ANÁLISIS DE RIESGOS

Establecer los riesgos a los cuales está propensa la Unidad de Estadística y Sistemas, de igual manera determinar el nivel o factor de riesgo, que lo clasificaremos en los siguientes:

Factor de Riesgo:

- Bajo
- Muy Bajo
- Alto
- Muy Alto
- Medio

Ellos nos determinan nuestra tabla de riesgos y nivel de factores que a continuación detallamos:

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 archivo.			X		
Terremotos, daño de equipos y archivos.					X
Acceso no autorizado, filtración de información					X
Robo de datos					X
Fraude, alteración de información.				X	
Desastre Total					X

En base a la tabla anteriormente presentada, concluimos que nuestro análisis de riesgo a modo general, nos hace ver que las posibles contingencias que pudieran presentarse en su mayoría van de un factor de ocurrencia medio y muy alto.

A continuación realizamos un deslinde de las causas por las cuales mayormente se presentan este tipo de contingencias, para ello realizamos la siguiente lista de preguntas:

1. Con respecto al **fuego**, que puede destruir los equipos y los archivos
   - ¿La Institución cuenta con protección contra incendios?
   - ¿Se cuenta con sistemas de aspersión automática?
   - ¿Cuenta con diversos extintores?
   - ¿Detectores de humo?
   - ¿Los empleados están preparados para enfrentar un posible incendio?

2. Con respecto al **robo común,** llevándose los equipos y archivos
   - ¿En qué tipo de vecindario se encuentra la Institución?
   - ¿Hay venta de drogas?
   - ¿Los equipos de cómputo se ven desde la calle?
   - ¿Hay personal de seguridad en la Institución?
   - ¿Cuántos vigilantes, están ubicados en zonas estratégicas?
   - ¿Existe un sistema de seguridad para prevenir el ingreso de personas no autorizadas?

3. Con respecto al **vandalismo,** que dañen los equipos y archivos
   - ¿Existe la posibilidad que un ladrón cause daños?
   - ¿Hay la probabilidad que causen algún otro tipo de daño intencionado?

4. Con respecto a **fallas en los equipos,** que dañen los archivos
   - ¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?
   - ¿Cuáles son las condiciones actuales del hardware?
   - ¿Es posible predecir las fallas a que están expuestas los equipos?

5. A **equivocaciones** que dañen los archivos
   - ¿Cuánto saben los empleados de computadoras o redes?
   - Los que no conocen del manejo de computadora, ¿saben a quién pedir ayuda?

- Durante el tiempo de vacaciones de los empleados, ¿Qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

6. Con respecto a la acción de **virus**, que dañen los archivos
   - ¿Se prueba software en la oficina sin hacerle un examen previo?
   - ¿Está permitido el uso de USB en la oficina?
   - ¿Todas las máquinas tienen puertos USB activos?
   - ¿Se cuentan con procedimientos contra los virus?

7. Con respecto a **terremotos,** que destruyen los equipos y archivos
   - ¿La Institución se encuentra en una zona sísmica?
   - ¿El edificio cumple con las normas antisísmicas?
   - Un terremoto, ¿cuánto daño podría causar?

8. Con respecto a **accesos no autorizados,** filtrándose datos importantes
   - ¿Existe registro de personal autorizado en la Municipalidad?
   - ¿Qué probabilidad hay que un colaborador intente hacer un acceso no autorizado?
   - ¿Existe comunicación remota de la red? ¿Qué tipo de servicio se utiliza (Telnet, FTP, etc.)?
   - ¿Contamos con Sistemas de Seguridad en el Correo Electrónico o Internet?

9. Con respecto al **robo de datos,** y la posible difusión de estos
   - ¿Cuánto valor tienen actualmente las Bases de Datos?
   - ¿Cuánta pérdida podría causar en caso de que se hicieran públicas?
   - ¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?

10. Con respecto al **fraude,** vía computadora
    - ¿Cuántas personas se ocupan de la contabilidad de la Institución?
    - ¿Los sistemas son confiables? ¿Pueden copiar datos en archivos?
    - Las personas que trabajan en las diferentes áreas, ¿qué tipo de antecedentes laborales tienen?
    - ¿Existe acceso a los sistemas desde otros sistemas externos o por personas no autorizadas?

B. PLAN DE RECUPERACIÓN DE DESASTRES

Ahora definimos las acciones a tomar para recuperarnos de la ocurrencia de un desastre. Este Plan de Recuperación contiene 3 etapas:

1. ACTIVIDADES PREVIAS AL DESASTRE

Como actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de información que nos asegure un proceso de recuperación con el menor costo posible a nuestra institución, tenemos que señalar las siguientes acciones que son precisas de realizar en la ejecución del presente plan.

a. Definición y Establecimiento de un Plan de Acción

Establecer los procedimientos relativos a:

(1). Sistemas de Información. La Unidad de Estadística y Sistemas tendrá una relación de los Sistemas de Información con los que cuenta. Debiendo identificar toda información sistematizada o manual, que sea necesaria para la buena marcha institucional.

La relación de Sistemas de Información detallará los siguientes datos:

- **Nombre del sistema,** es determinado por el analista-desarrollador asignado por la Unidad de Estadística y Sistemas
- **Lenguaje o Paquete,** con el que fue creado el Sistema, programas que lo conforman (tanto programas, fuentes como programas objetos, rutinas, macros, etc.)
- **La Dirección,** (Gerencia, SubGerencia, Oficina, Unidad, etc.) que genera la información base (el <<dueño>> del sistema.)
- Las **unidades o departamentos** (internos/externos) 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 de Información (actividades de Restore)

Con toda esta información se realizará una lista priorizada (Ranking) de los Sistemas de Información necesarios para que la Municipalidad Provincial de Barranca recupere su operatividad perdida en el desastre (Contingencia)

(2). Equipos de Cómputo: Se tendrá en cuenta lo siguiente:

- **Inventario actualizado** de los equipos de manejo de información (computadoras, 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 hará 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 PCs con información importante o estratégica y color verde a las PCs de contenidos normales.

- **Respaldo de PC's,** tener siempre una relación actualizada de PC's requeridas como mínimo para cada sistema permanente de la institución (que por sus funciones constituye el eje central de los servicios informáticos), para cubrir las funciones básicas y prioritarias de cada uno de estos sistemas cuando se requiera.

(3). Obtención y Almacenamiento de los Respaldos de Información (Backups):
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 Municipalidad Provincial de Barranca, contando 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 objeto correspondiente, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final. Considerando las copias de los listados fuentes de los programas definitivos, para casos de problemas.
- **Backups de los Datos.** Base de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del software aplicativo de la MPB.
- **Backups del Hardware.** Implementar mediante 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.** Teniendo dos locales, 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.

(4) Políticas (Normas y Procedimientos de Backups): Establecer los procedimientos, normas y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente en el punto 3). Incluyéndose:

- Periodicidad de cada tipo de Backups.
- Respaldo de Información de movimiento entre los periodos que no se cuenta con Backups (backups incrementales)
- Uso obligatorio de un formulario estándar para el registro y control de backups.
- Correspondencia entre la relación de sistemas e informaciones necesarias para la buena marcha de la institución (mencionado en el punto a) 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 medo magnético de soporte se pueda deteriorar (reciclaje)
- Pruebas periódicas de los Backups (Restores), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

b. Formación de Equipos Operativos para el Plan de Acción

Todas las áreas u oficinas de la MPB, que almacenen información y que sirva para la operatividad institucional, designará un responsable de la seguridad de dicha información. Pudiendo ser el jefe del área o el colaborador que maneje directamente la información.

Entre las acciones a tomar por la Unidad de Estadística y Sistemas conjuntamente con las oficinas 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, subsistemas.
- Supervisar procedimientos de respaldo y restauración.
- Supervisar la carga de archivos de datos de las aplicaciones y la creación de respaldos incrementales.
- Coordinar líneas, terminales, routers, otros aditamentos para comunicaciones.
- Establecer procedimiento 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.
- Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- Participar en las pruebas y simulacros de desastres.

- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.

2. ACTIVIDADES DURANTE EL DESASTRE

Una vez presentada la contingencia, se ejecutará las siguientes actividades:

a. Plan de Emergencia

Establecer las acciones que se deben realizar cuando se presente un siniestro, así como la difusión de las mismas.

Conviene prever los posibles escenarios de ocurrencia del Siniestro:

- Durante el día
- Durante la noche o madrugada

Este plan incluirá la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre la contingencia.

Si bien es cierto la integridad de las personas es lo primordial, se deben adoptar medidas con el fin de asegurar la información, detallando:

- Vías de salida o escape.
- Plan de Evacuación de Personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de información) de la MPB (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/ambulancias, Jefatura de Seguridad Ciudadana, Comisaría PNP y de su personal (equipos de seguridad) nombrados para estos casos.

  En caso de contingencias como fallas en equipos de cómputo, fallas humanas, acción de virus, etc.; solicitar la ayuda del personal de la Unidad de Estadística y Sistemas si es que en el área no existe una persona capacitada para resolver el problema

b. 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, para salvar los equipos señalados en el acápite B.1.a. (Definición y Establecimiento del Plan de Acción).

c. Entrenamientos

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se le hayan

asignado en los planes de evacuación de personal o de equipos para minimizar costos, se puede aprovechar las fechas de recarga de extinguidores o las charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de los siniestros (incendios, inundaciones, terremotos, apagones, y/o atentados terroristas, etc.) pueden realmente ocurrir y tomar con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los gerentes, subgerentes, jefes de la MPB, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

3. ACTIVIDADES DESPUÉS DEL DESASTRE

Durante la contingencia, se tomará en cuenta lo planificado en el plan de Emergencia.

a. Evaluación de Daños

Inmediatamente después que la contingencia ha concluido, se evaluará la magnitud de los daños producidos, estableciendo que sistemas están afectados, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se lanzará 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.

b. Priorización de actividades del Plan de Acción

Toda vez que el Plan de acción contemple una pérdida total, la evaluación de daños reales y su comparación con el Plan, nos dará la lista de actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra institución.

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

c. 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 contará con un coordinador que reportará diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, informará de inmediato a la jefatura a cargo del Plan de Contingencias (Unidad de Estadística y Sistemas).

Los colabores de recuperación tendrán dos etapas:

- **La primera**, la restauración de los servicios usando los recursos de la MPB o local de respaldo.
- **La segunda,** es volver a contar con los recursos en las cantidades y lugares propios de los sistemas 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 MPB o local de respaldo.

d. Evaluación de Resultados

Una vez concluidas las labores de recuperación del (los) sistema(s) que fueron afectados por la contingencia, se evaluará 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, saldrán 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.

e. Retroalimentación del Plan de Acción

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

CAPITULO III

FASE DE ORGANIZACIÓN DE UN SISTEMA DE ALERTA CONTRA FALLAS

La importancia del sistema de alertas es vital para identificar las fallas, las magnitudes de las mismas y poder establecer acciones correlativas o de contingencia necesaria.

A. DISEÑO DEL SISTEMA DE ALERTAS

La alerta, es el estado anterior a la ocurrencia de un desastre o falla, que se declara con el fin de que los organismos de emergencia activen procedimientos de acción preestabiecidos (acciones de contingencia) y para que se tomen las precauciones específicas en las dependencias afectadas, debido a la inminente ocurrencia de un evento previsible.

El establecimiento de alertas antes de la ocurrencia de un evento, depende de la predicción que pueda hacerse de la falla originaria del desastre.

1. Definición de Alerta

La alerta es como el aviso o señal que se da, para que se sigan instrucciones específicas debido a la presencia real o inminente de un evento peligroso. Estas alertas pueden ser sonoras o luminosas.

2. Estados de Alerta

Dependiendo del nivel de certeza que se tiene de la ocurrencia del evento se puede definir diferentes estados de alerta. Usualmente, cuando el desastre lo permite, se utilizan tres estados que, de acuerdo con la gravedad de la situación significa para las instituciones el aislamiento, la movilización y respuesta.

En ocasiones dichos estados son identificados mediante colores o nombres que no solo se utilizan para informar de una manera práctica acerca de la inminencia de un evento, sino también para demarcar las áreas de influencia del mismo.

3. Procesos que se dan en las organizaciones para todo estado y nivel de alerta.

Es importante mencionar que durante un tiempo prolongado de alerta, los niveles o estados de la misma no deben estar cambiándose continuamente, y que un estado de alerta de máxima atención no debe ser adoptado por mucho tiempo, debido a que este tipo de situación genera una reacción negativa en la organización afectada y de las instituciones.

4. Cambio de alerta

Nos implica una modificación significativa de la actuación institucional o del comportamiento del servicio no tiene razón de ser y se presta para la confusión.

Un cambio de alerta normalmente es sugerido o recomendado por la Unidad de Estadística y Sistemas, sin embargo, es usual que el cambio sea decidido por las gerencias/oficinas de las áreas, excepto en el caso de que, por la ocurrencia repentina de un evento peligroso, sea necesario activar alarmas que indican dicha situación sin previa concertación o consulta.

Los cambios de alerta comúnmente se realizan a través de los medios de comunicación internos de la MPB, sin embargo en algunos casos también se utilizan alarmas, que son señales sonoras o de luz que emiten para que se adopten instrucciones preestablecidas de emergencia.

B. ROLES Y RESPONSABILIDADES

La implantación de un sistema de contingencias, alerta y soporte frente a las contingencias derivadas de fallas originadas de las mismas, implica disponer de una organización de personal con responsabilidades bien definidas y recursos, para poder suplir los sistemas que pudieran ser afectados.

ORGANIZACIÓN	RESPONSABILIDAD EN EL PLANEAMIENTO DE CONTINGENCIAS
Comité técnico institucional	Planifica, programa y evalúa las medidas de adaptación y contingencia.
UES	Desarrolla, monitorea, organiza y da mantenimiento al Plan de Contingencia. Brinda servicio de soporte preliminar a las áreas de trabajo afectadas por algún siniestro o contingencia.
Equipo de Recuperación de Desastres – ERD	Forma parte de la Unidad de Estadística y Sistemas ejecuta la recuperación de los sistemas, equipos y/o servicios cuando estos han fallado.
Supervisores de Área de Trabajo	Controla las operaciones de un área de trabajo específica, participa accionando el plan de contingencias, en el caso que los sistemas a su cargo no puedan operar normalmente y no se pueda recuperar la operatividad de los mismos.
Usuarios Finales	Es el usuario de los sistemas informáticos y tecnológicos utilizados por la Municipalidad.

Ahora describiremos las responsabilidades de cada rol:

1. Área de Seguridad (UES)

El área organizacional encargada de la administración de seguridad de la información tiene como responsabilidades:

a. Establecer y documentar las responsabilidades de la Municipalidad en cuanto a seguridad de información.
b. Mantener la política y estándares de seguridad de información de la Municipalidad.
c. Identificar objetivos y estándares de seguridad de la Municipalidad (prevención de virus, uso de herramientas de monitoreo, etc.)
d. Definir metodologías y procesos relacionados a la seguridad de información.
e. Comunicar aspectos básicos de seguridad de información a los trabajadores de la Municipalidad. Esto incluye un programa de concientización para comunicar aspectos básicos de seguridad de información y de las políticas de la Municipalidad.
f. Desarrollar controles para las tecnologías que utiliza la Municipalidad. Esto incluye el monitoreo de vulnerabilidades documentadas por los proveedores.
g. Monitorear el cumplimiento de la política de seguridad de la Municipalidad.
h. Controlar e investigar incidentes o violaciones de seguridad.
i. Realizar una evaluación periódica de vulnerabilidades de los sistemas que conforman la red de datos de la Municipalidad.
j. Asistir a las gerencias en la evaluación de seguridad de las iniciativas del negocio.
k. Verificar que cada activo de información de la Municipalidad haya sido asignado a un "propietario" el cual debe definir los requerimientos de seguridad como políticas de protección, perfiles de acceso, respuesta ante incidentes y sea responsable final del mismo.
l. Administrar un programa de clasificación de activos de información, incluyendo la identificación de los propietarios de las aplicaciones y datos.

m. Coordinación de todas las funciones relacionadas a seguridad, como seguridad física, seguridad de personal y seguridad de información almacenada en medios no electrónicos.
n. Desarrollar y administrar el presupuesto de seguridad de información.
o. Administración de accesos a las principales aplicaciones de la Municipalidad.
p. Elaborar y mantener un registro con relación de acceso de los usuarios sobre los sistemas y aplicaciones de la Municipalidad y realizar revisiones periódicas de la configuración de dichos accesos en los sistemas.
q. Controlar aspectos de seguridad en el intercambio de información con entidades externas.

2. Custodio de Información

Es el responsable de la administración diaria de los sistemas de información y el monitoreo del cumplimiento de las políticas de seguridad en los sistemas que se encuentran bajo su administración.

Sus responsabilidades son:

a. Administrar el acceso a nivel de red (sistema operativo)
b. Administrar acceso a nivel de base de datos
c. Administrar los accesos a los archivos físicos de información almacenada en medios magnéticos (cintas), ópticos (CD's), USB o impresa.
d. Implementar controles definidos para los sistemas de información, incluyendo investigación e implementación de actualizaciones de seguridad de los sistemas (service packs)
e. Desarrollar procedimientos de autorización y autenticación.
f. Entrenar en nuevas tecnologías o sistemas implantados bajo su custodia.
g. Asistir y administrar los procedimientos de backup, recuperación y plan de continuidad de sistemas.

3. Usuario

La responsabilidad de los usuarios finales, es decir, aquellas personas que utilizan información de la Municipalidad como parte de su trabajo diario están definidas a continuación:

a. Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas.
b. Reportar supuestas violaciones de seguridad de información.
c. Asegurarse de ingresar información adecuada a los sistemas.
d. Adecuarse a las políticas de seguridad de la Municipalidad.
e. Utilizar la información de la Municipalidad únicamente para los propósitos autorizados.

4. Propietarios de la información

Los propietarios de la información son los gerentes, subgerentes, jefes de oficina, de unidades de la Municipalidad, los cuales, son responsables de la información que se genera y se utiliza en las operaciones. Todas las áreas deben ser conscientes de los riesgos de tal forma que sea posible tomar decisiones para disminuir los mismos.

Entre las responsabilidades de los propietarios de información se tienen:

a. Asignar los niveles iniciales de clasificación de información.
b. Revisión periódica de la clasificación de la información.

c. Asegurar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
d. Determinar los criterios y niveles de acceso a la información.
e. Revisar periódicamente los niveles de acceso a los sistemas a su cargo.
f. Determinar los requerimientos de copias de respaldo para la información que les pertenece.
g. Tomar las acciones adecuadas en caso de violaciones de seguridad.
h. Verificar periódicamente la integridad y coherencia de la información producto de los procesos de su área.

C. SISTEMA DE COMUNICACIÓN Y ALERTAS

Predecir un evento es determinar con certidumbre cuándo, dónde y de qué magnitud será dicho evento, lo cual, con el estado actual del conocimiento, no es posible lograr para todos los elementos que pueden generar el desastre. La investigación científica y la instrumentación mediante redes de vigilancia y monitoreo permiten en algunos casos predecir o detectar contingencias, que dependiendo de la certeza o del tiempo que tardan sus efectos en ser sentidos en un sitio, dan la posibilidad de declarar estados de alerta y/o de alarma para la protección y/o evacuación del ente. El establecimiento de alarma antes de la ocurrencia de un evento, depende de la predicción que pueda hacerse del desastre.

1. Preparativos para la respuesta

Es evidente que si se acepta que existe riesgo en algún grado, significa que existe la posibilidad de que se presente una falla, desastre o contingencia, aun cuando en algunos casos debidos a las acciones de prevención y de mitigación, se logrará reducir su probable ocurrencia. Por lo tanto en la etapa de preparación debe estructurarse la respuesta para la atención de las emergencias que eventualmente se pueden presentar reforzando así las medidas de mitigación o reducción de sus efectos.

La preparación se lleva a cabo mediante la organización y planificación de las acciones de alerta, búsqueda, detección y asistencia que deben realizarse en casos de emergencia. Por esta razón, en esta etapa deben considerarse aspectos tales como la predicción de eventos, la educación y capacitación del personal a cargo, el entrenamiento de los organismos de emergencia y la organización y coordinación para la respuesta en caso de falla o desastre.

Es importante que en esta etapa se tenga en cuenta la iniciativa y la capacidad de la organización potencialmente afectado para enfrentar por sus propios medios las consecuencias de los desastres, y por lo tanto la efectividad que tiene que llevar a cabo anticipadamente actividades de capacitación, educación e información como refuerzo a la capacidad de reacción espontánea del ente.

La declaración de alerta, particularmente en caso de situaciones de máxima atención o alarma, debe ser:

- Accesible, es decir debe difundirse por muchos medios.
- Inmediata, puesto que toda demora puede interpretarse en el sentido de que el peligro no es real o inminente.
- Coherente, es decir no debe haber contradicciones.
- Oficial, es decir que procesa de fuentes que son normalmente aceptadas o fiables.

Por su contenido y su forma los mensajes de máxima alerta o alarma deben ser:

- Concretos, deben dar una información clara sobre la amenaza.
- Apremiantes, deben promover la acción inmediata de la organización bajo riesgo.
- Significa advertencia, deben expresar las consecuencias de no atender la alerta.

2. Instrumentos para la vigilancia.

Para las alertas son las redes, vigilancia, monitoreo e investigación, los sistemas de alarma y los medios de comunicación. Estos sistemas pueden ser de alcance internacional, nacional, regional o local.

Son instrumentos que son utilizados para el funcionamiento de algunos sistemas de alerta:

- Redes de vigilancia y monitoreo.
- Imagen de satélite, sensores remotos y teledetección.
- Sistema de sirenas, altavoces y luces.
- Medios de comunicación con mensajes pregrabados
- Redes de comunicación inalámbrica – sistema de télex, fax y teléfono.

D. EL SISTEMA DE ALERTA Y LOS PROCEDIMIENTOS DE CONTINGENCIAS

El objetivo fundamental del sistema de alerta (la respuesta) es lograr salvar el normal funcionamiento de los servicios involucrados, reducir el impacto y proteger los bienes. Significando que la respuesta es la ejecución de acciones de búsqueda, detección y asistencia que se llevan a cabo debido a la ocurrencia de un desastre o ante la inminencia del mismo.

Dado que las emergencias pueden ser de orden local, regional o nacional dependiendo si los límites territoriales son rebasados por el evento o por que la movilización y el empleo de recursos superan las capacidades de cada nivel, la respuesta de igual forma podrá ser de orden local, regional o nacional. Los instrumentos de la etapa de respuesta corresponden necesariamente a las actividades que los planes indican que deben ejecutarse en caso de un desastre o contingencia.

E. LINEAMIENTOS EN LOS QUE SE BASA LA ORGANIZACIÓN DE UN SISTEMA DE ALERTAS

1. Establecer un código de señales para contingencias.
2. Establecer los puntos de control de los diversos sistemas de las MPB
3. Implementar un sistema de comunicación a prueba de fallas en la MPB
4. Entrenamiento de los colaboradores para interpretar las señales de alerta.
5. Organizar a los colaboradores para actuar ante la aparición de las contingencias
6. Establecer los mecanismos necesarios para poner en operación el plan de contingencias

CAPITULO IV

ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACION

A. CONCEPTOS GENERALES

1. Privacidad

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

2. 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.

3. 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.

4. 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), hoja de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

5. 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.

6. Acceso

Es la recuperación o grabación de 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.

7. Ataque

Término 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.

8. 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. Ejemplo: el borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

9. Ataque Pasivo

Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico 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.

10. Amenaza

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Falas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

11. Incidente

Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

12. Golpe (Breach)

Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

CAPITULO V

AMENAZAS MÁS COMUNES CONTRA LA SEGURIDAD

A. EL FUEGO

El fuego es un elemento comprendido dentro de las principales amenazas contra la seguridad. El fuego es un problema crítico en un centro de cómputo por varias razones: primero, porque el centro está lleno de material combustible como papel, cajas, etc. El hardware y el cableado del suelo falso pueden ser también fuentes de serios incendios. Desgraciadamente los sistemas anti fuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputo.

El fuego es considerado el principal enemigo del computador ya que puede destruir fácilmente los ficheros de información y programas.

Es necesario e imprescindible implementar en la MPB un sistema que nos permita en primer lugar detectar la posible ocurrencia de un siniestro de este tipo en cualquiera de los ambientes de la Municipalidad y así mismo sofocar el fuego en el caso de producirse.

B. EXTINGUIDORES MANUALES

Muchas veces el contar con sistemas automáticos antifuego (sprinklers de agua o sistemas de rociado de gas) no es debido a su alto costo, entonces se debe actuar con rapidez para poder sofocar el incendio. Para ello se debe tener en cuenta del material que se está siendo consumido por el fuego. Para cada tipo de situación hay un agente antifuego ideal, así tenemos:

	Gas Carbónico (CO_2)	Espuma	Agua
Papel Madera Este tipo de material que deja brasa o ceniza requiere un agente de moje o enfrie	Apaga solamente en la superficie	Sofoca	Excelente enfría y empapa, apaga totalmente
Equipamiento Eléctrico	Excelente, no deja residuos, no daña el equipamiento y no es conductor de electricidad	Conduce la electricidad y además daña el equipo	Conductora de electricidad
Líquidos Inflamables (aceites, gasolina, grasa, etc.) Requiere acción rápida de sofocar y enfriar	Bueno, no deja residuos y es inofensivo	Excelente, produce una sabana de espuma que sofoca y enfría	

Material	Modo de Operarios
CO2	1. Retirar la trabaja de seguridad 2. Asegure firmemente el mango difusor 3. Apretar el gatillo 4. Oriente el chorro hacia la base del fuego haciendo un barrido **Alcance:** 1 a 2 metros **Sustancia:** Bióxido de carbono **Momento del Recargo:** Pérdida del mas de 10% o más del peso
Polvo Químico	1. Abra la ampolla de gas. 2. Asegure firmemente el mango difusor 3. Apretar el gatillo 4. Oriente el chorro de manera de crear una cortina de polvo sobre el fuego. **Alcance:** de 2 a 4 metros Sustancia: Polvo Químico seco y CO2 producido por el contacto del polvo con fuego. Momento de Recargo: Pérdida de peso de la ampolla superior al 10%
Espuma	1. Inversión del aparato para abajo 2. Oriente el chorro para la base del fuego Alcance: de 9 a 18 metros Sustancia: Espuma formada por burbujas consistentes llenas de CO2 Momento del Recargo: Anualmente
Agua - Gas	Simple maniobra de apertura a la ampolla de CO2 que sirve de propagador. Alcance: de 9 a 20 metros Sustancia: Agua Momento de recargo: Anualmente

Instrucciones

Los colabores designados para usar extinguidores de fuego deben de ser entrenados en su uso. Ellos deben recibir algunas lecciones de instrucciones en el mecanismo de lucha contra el fuego y luego estar entrenados de cómo opera el extinguidor de mano.

Es muy importante que todos los colaboradores reciban la instrucción de no interferir con este proceso y evitar su actuación en el sistema de extinción.

Muchas veces la sensibilidad de comienzo de fuego en los ambientes laborales es muy alta. Esto genera falsas alarmas y los colaboradores se acostumbran a fomentar el pánico, sin observar realmente si hay fuego.

Ello implica tener en cuenta algunos detalles más como son:

- Cuidado al seleccionar e implementar los sistemas de extinción y su conexión si es efectuada con fuerza eléctrica
- Tener a mano el número telefónico de la Compañía de Bomberos y demás números de emergencia.
- Mantener procedimientos planificados para recibir y almacenar abastecimientos de papel.

C. EL AGUA

Otro de los peligros relevantes es el agua. El agua puede entrar en una sala de computadores por varios conductos.

Realmente el agua es una amenaza para los componentes del computador y cables.

Los daños por agua pueden ocurrir como resultado de goteo del techo, inundación de baños interiores, inundaciones por lluvias, goteos de tuberías del techo, filtraciones de agua y de operaciones de sistemas de regadío en pisos sobre oficinas. Es necesario entonces que el equipo así como los muebles y cabinas cuenten con protección contra

agua y trazar un plan para la rápida eliminación de algo de agua que podría entrar en el área.

Poner atención en la instalación de desagües bajo el piso construido donde están instalados los sistemas de cables. La conveniencia de cubiertas plásticas es necesaria en la protección del equipo contra el agua, procedente de filtraciones a través del techo.

D. INSTALACIONES ELÉCTRICAS

Para que funcionen adecuadamente, las computadoras personales necesitan de una fuente de alimentación eléctrica fiable, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible.

Las computadoras personales toman la electricidad de los circuitos eléctricos domésticos normales, a los que se llama tomas de corriente. Esta corriente es bastante fuerte, siendo una corriente alterna (ac) ya que alterna el positivo con el negativo. La mayor parte de las computadoras personales incluyen un elemento denominado **fuente de alimentación**, la cual recibe corriente alterna de las tomas de corriente y la convierte o transforma en la corriente continua de baja potencia que utilizan los componentes de la computadora.

La fuente de alimentación es un componente vital de cualquier computadora personal, y es la que ha de soportar la mayor parte de las anomalías del suministro eléctrico. Actualmente existe el concepto de fuente de alimentación redundante, la cual entrará en operación si se detecta una falla en la fuente de alimentación principal.

En nuestro medio se han podido identificar siete problemas de energía más frecuente:

1. Fallas de energía.
2. Transistores y pulsos
3. Bajo voltaje
4. Ruido electromagnético
5. Distorsión
6. Alto voltaje
7. Variación de frecuencia

Existen dispositivos que protegen de estas consecuencias negativas, los cuales tienen nombres como:

1. Supresores de picos
2. Estabilizadores, y
3. Sistemas de alimentación ininterrumpida (SAI o UPS: UNINTERRUPTIBLE POWER SISTEM)

E. FALLAS QUE GENERAN ALTAS TEMPERATURAS

La electricidad llega desde la central eléctrica hasta los enchufes de la oficina, sale por el hilo activo y a continuación vuelve a la central a través del neutro, tras haber realizado su trabajo. Los materiales a través de los cuales la electricidad fluye libremente, como es el cobre de los cables de la oficina, se denominan conductores. La electricidad es esencialmente perezosa, intentando volver a la central eléctrica lo más rápidamente posible a través de cualquier conductor disponible.

Lo que impide que la electricidad vuelva demasiado pronto es el aislamiento, el cual impide el paso de la electricidad. La goma, el plástico y una gran cantidad de materiales no metálicos son buenos aislantes. Por ejemplo la carcasa de algunas computadoras está hecha de metal conductor, pero si se toca ésta no da una descarga eléctrica, porque los aislantes mantienen la corriente dentro de los componentes internos del sistema.

Las fallas en los circuitos eléctricos se producen a menudo por un aislante o un conductor que no trabaja adecuadamente, generando inconvenientes, por lo general, altas temperaturas. Existen formas de prever estas fallas y tecnologías para minimizar el impacto de éstas; como por ejemplo:

1. **TOMAS DE TIERRA**

   Es la comunicación entre un circuito eléctrico y el suelo natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. También se le llama puesta a tierra. La comunicación con tierra se logra mediante la conexión de un circuito dado (tomacorriente) a un conductor, en contacto con el suelo. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en la tierra húmeda, con o sin agregados de ciertos componentes como carbón vegetal, sal o elementos químicos ("laborgel",etc), según especificaciones técnicas indicadas para las instalaciones eléctricas.

   Objetivo. Puede ser de distintos tipos. En la práctica sirve para proteger de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y, para disipar sobretensiones de origen atmosférico o de origen industrial, ya sea por maniobra o por pérdida de aislamiento.

   La toma a tierra limita la tensión que, con respecto a tierra, puede aparecer en cualquier elemento conductor de una instalación y asegura con ello la correcta actuación de los dispositivos de protección de la instalación eléctrica.

   Funciones. Cumplirá las siguientes:

   - Proteger a las personas, limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas.
   - Proteger los equipos y materiales, asegurando la educación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales.
   - Facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

   Partes. Consta de las siguientes:

   - Toma de Tierra o Puesta a Tierra
   - Línea principal de tierra
   - Derivaciones de las líneas principales de tierra.
   - Conductores de protección.

   Mantenimiento. Las inspecciones deben realizarse anualmente, con el fin de comprobar la resistencia y las conexiones. Esta labor se efectuará en los meses de verano o en tiempo de sequía, con el fin de evaluarlas en el momento más crítico del año por falta de humedad.

   El mantenimiento preventivo será de 3 a 4 años dependiendo de las propiedades electroquímicas estables.

2. FUSIBLES

Al cablear la computadora, la carcasa normalmente se conecta a la tercera patilla del cable de alimentación. En algunos casos, puede que la tierra se conecte también al neutro. Si la electricidad pasara a través del aislante y llegase a la carcasa, entonces pasaría directa desde el conductor de tierra hasta ésta. Simultáneamente, esta derivación de electricidad aumentaría la intensidad de corriente que va por el circuito. Este incremento puede ser detectado por un fusible o un diferencial. Estos dos dispositivos están diseñados para interrumpir un circuito si se sobrecargan (Un fusible debe ser sustituido tras fundirse, mientras que un diferencial se debe restaurar tras saltar).

Si una parte de una computadora funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo. A continuación debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible. Arreglado el problema, se puede volver a conectar el equipo. Vuelva a encender el equipo, pero esté preparado para tener que apagarlo de nuevo, y rápidamente, si el problema no se hubiera arreglado adecuadamente. Entre las causas menos problemáticas para que se fundan los fusibles o salten los diferenciales se encuentra la sobrecarga de un circuito eléctrico. Para corregir esto se necesita reorganizar la distribución de enchufes sobre las placas, distribuyendo la carga de forma más uniforme.

Entre las fallas más serias, se incluyen los cables dañados de forma que el asistente entre los conductores se ha roto. En los aparatos, los aislantes pueden decaer o fundirse, dando lugar a cortocircuitos. Al sustituir los fusibles de una computadora, se ha de tener cuidado que todos los equipos deben estar apagados y desconectados antes de cambiar el fusible. No se debe olvidar que algunos elementos del equipo, como es el caso de los monitores, pueden mantener una carga de alto voltaje incluso, después de haberse apagado.

Debe asegurarse que el fusible de recambio es de la misma capacidad que el fundido. Por ejemplo, si el fusible fundido viene marcado como de 2 amperios, no se debe sustituir por uno de 3 amperios. Un fusible de 3 amperios dejará pasar 1 amperio más de intensidad de lo que fijó el diseñador del equipo. Si se siguen fundiendo fusibles en el equipo, entonces hay algo que funcional mal. No se apruebe las reparaciones de los fusibles, usando hilos de cobre o similares.

3. EXTENSIONES ELÉCTRICAS Y CAPACIDADES

Las computadoras personales a veces ocupan rápidamente todas las tomas de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado por los responsables de las oficinas. No sólo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. Aparte del daño físico que puede provocar engancharse repentinamente con el cable, se trata de una forma rápida y poco agradable de desconectar un sistema completo.

Por razones de seguridad física y de trabajo se sugiere tener en cuenta las siguientes reglas:

- Las extensiones eléctricas deben estar afuera de las zonas de paso, siempre que sea posible.

- Se debe utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.
- No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase más corriente de la que los cables están diseñados para soportar. Utilice los enchufes de pared siempre que sea posible.
- Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar a limitar el daño ante fallas eléctricas.
- Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esa cifra el amperaje total de todos los aparatos conectados a ellas.
- Adquiera toma corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar tanto con enchufes de patas planas, como cilíndircas.
- Tanto los toma corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

F. CAÍDAS Y SUBIDAS DE TENSION

Las caídas y subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras personales, los monitores, las impresoras y los demás periféricos.

Lo que causa problemas en las computadoras personales son las grandes oscilaciones en el voltaje. Por ejemplo, una caída por debajo de los 200V y una subida por encima de los 240V. Si una caída dura más de una fracción de segundo, puede generar una falta de alimentación a la memoria de acceso aleatorio, con lo que los datos que allí se encuentren, pueden perderse o, como mínimo, resultar desordenados. Es más, el efecto de la vuelta de la corriente a su valor normal puede tener también efectos perniciosos.

Los efectos de una subida son difíciles de predecir, dependiendo hasta cierto punto de la fuente de alimentación de la computadora. Esta tiene un efecto moderador sobre subidas de la corriente, pero puede que no sea suficiente para evitar cortes temporales en los circuitos que lleven a que se desordenen los datos o incluso se dañen los circuitos impresos. Un comportamiento errático es el primer síntoma de una subida de tensión.

Si se es cuidadoso, es bastante aconsejable medir el voltaje. Un típico multímetro digital, dará una medición del voltaje si introduce sus terminales en el enchufe.

Si la lectura del voltaje continúa fluctuando, anote la medida más alta y la más baja. Si se encuentran dentro de un margen del 5 por 100, alrededor del voltaje esperado, probablemente no causará ningún problema. Si las oscilaciones se encuentran fuera de este margen, puede ser recomendable pedir que un electricista revise el cableado e invertir en algún equipo de acondicionamiento de corriente (Estabilizadores de Voltaje)

1. SUPRESORES DE SUBIDAS DE TENSIÓN

Una protección relativamente barata ante las subidas de tensión es un supresor de subidas. Este es un dispositivo eléctrico situado entre la computadora personal y la fuente de corriente. Incluye una circuitería electrónica que recorta el voltaje cuando éste comienza a subir por encima de un nivel aceptable. El supresor de subidas evita que las subidas de la corriente de alimentación peligrosas lleguen al equipo.

La circuitería del supervisor de subidas es bastante compacta, por lo que estas unidades pueden encontrarse con distintas formas y tamaños. Cualquier buen supresor de subidas de tensión debe contar con las siguientes características:

a. Ruptor de circuito

Cualquier supresor de sobretensiones debe incluir un ruptor del circuito, un conmutador rearmable que corta la alimentación si se sobrecargan los circuitos (normalmente un switch). Este es el mismo nivel de protección para cualquier dispositivo, debiendo incluso la extensión eléctrica múltiple más sencilla, de incluir uno. También cabe señalar el hecho de que una extensión eléctrica múltiple tenga un ruptor, no lo convierte en un supresor de sobretensiones. Se ha de señalar que si un ruptor ha saltado, no se debe rearmar (apretar el switch) hasta que no se haya determinado primero la causa que lo hizo saltar.

b. Protección separada

Muchos supresores de subidas de tensión ofrecen varios puntos de conexión para conectar el sistema. El diseño de la unidad debe proteger cada punto de conexión de forma separada. Con este diseño es fácil que pueda hacer frente a subidas más grandes que con otro en que simplemente se protege la línea que va al múltiple. La protección separada también puede contribuir a reducir la interferencia de ruido entre los distintos elementos conectado al mismo circuito de alimentación.

c. Medidas

Se puede encontrar distintas medidas relativas a los supresores de subidas de tensión en la documentación que traen. Una medida básica es la capacidad, en términos de la corriente total que el dispositivo está diseñado para proteger. Esta medida tiene aquí el mismo significado que para una extensión eléctrica múltiple. Si éste o el supresor presentan un valor de 10 amperios, en ese caso el total de intensidad de todos los equipos conectados al elemento no debe superar esa cantidad. El voltaje se cierre inicial es la tensión a la que se produce el efecto de cierre de la circuitería del elemento.

2. PICOS

Una variación en la corriente más peligrosa y difícil de medir son los picos. Estos consisten en una subida de tensión a niveles muy altos. Muchos de estos picos son causados por la conexión y desconexión de grandes aparatos eléctricos. Los picos son de dos tipos distintos:

- Modo Normal y
- Modo Común

Los sucesos de modo normal se pueden medir entre los hilos activo y neutro del circuito eléctrico del edifico. Los de modo común se miden entre el neutro y la tierra. Un pico en modo normal de gran magnitud puede dañar la fuente de alimentación de la microcomputadora. Sin embargo, un pico en modo común de solo unas pocas docenas de voltios puede dañar los circuitos lógicos o producir errores entre las computadoras.

Protección frente a Picos. Los circuitos supresores de sobretensiones ofrecen buena protección frente a picos en modo normal, pero podría causar algunos de modo común. Por ello, muchos supresores de sobretensión también poseen una circuitería para bloqueo de picos separada, y se comercializan como protectores para sobretensiones y picos.

Los criterios de adquisición de un protector ante picos son en gran parte los mismos que los de los protectores ante sobretensiones, **siendo normal y deseable que una misma entidad ofrezca protección ante ambos**, aunque se debe comprobar sus especificaciones para asegurarse. La capacidad de impedir que los picos alcancen el equipo a veces se miden en *julios*.

Un *julio* es una medida de energía, la energía consumida durante cierto periodo de tiempo, así por ejemplo, un producto puede venir con la especificación de que suprime picos de 140 julios. También puede venir con una especificación en amperios, como sería "picos de 140 julios a 6500 amperios". Por lo general, cuando mayor sea el voltaje-julios-amperios que el protector puede tratar, se considera mejor.

G. RUDIO ELECTRÓNICO

Las subidas y caídas de tensión y los picos no son el único problema eléctrico al que han de enfrentar los usuarios de computadoras. También está el tema del Ruido, no se trata del que se puede oír, sino del ruido eléctrico que interfiere en el funcionamiento de los componentes electrónicos.

Para describir el ruido se utilizan dos términos:

- Interferencia de radiofrecuencia (RFI)
- Interferencia electromagnética (EMI)

Este ruido se puede ver literalmente cuando se utiliza un taladro eléctrico cerca de un televisor. El motor eléctrico del taladro hará que aparezcan líneas, nieve u otras alteraciones en la pantalla. Una interferencia similar puede ser causada por las bujías de un automóvil. También puede generarse interferencia de radio con teléfonos inalámbricos que utilizan ondas de radio para comunicar entre la unidad móvil y la base. No sólo la recepción de la TV, sino también la integridad de los datos dentro de una computadora están en peligro ante éstas y otras fuentes de interferencia.

Las computadoras personales corren el riesgo de sufrir tanto interferencias externas como emisiones electromagnéticas y de radio creadas por las propias computadoras. Muchos de los circuitos de una computadora generan EMI y RFI.

El ruido eléctrico también afecta a las transmisiones telefónicas. Se pueden conseguir filtros para las líneas telefónicas que realizan transmisión de datos y fax. En algunos casos, éstos vienen combinados con supresores de subidas de tensión y picos. La línea de teléfono de la pared se acopla a la unidad supresora, y a continuación se conecta el teléfono – modem – fax a la unidad, quedando la línea telefónica filtrada y protegida.

El otro aspecto de los problemas de ruido con el teléfono es la interferencia de los teléfonos con las computadoras personales.

Esto ocurría a menudo con los primeros teléfonos inalámbricos, pudiendo ser necesario tener la unidad de base del teléfono inalámbrico lejos de la computadora.

Protección ante el Ruido

Para proteger las computadoras de las interferencias electromagnéticas y de radio frecuencia es necesario considerar lo siguientes:

- **Ruido en la línea de alimentación**
  Algunos supresores de subidas de tensión y picos están diseñados con una circuitería que filtra el ruido de la fuente de alimentación. La supresión del ruido se mide en decibeles.

- **Situación de los Aparatos**

  Como regla general se puede decir que las computadoras personales y los aparatos eléctricos de gran consumo no congenian. Cuando se instalan puestos de trabajo con computadoras se debe intentar tenerlos lejos de estos equipos. Es difícil suprimir la interferencia generada por las potentes corrientes que circulan por estas máquinas, como son las grúas, ascensores, prensas de imprenta y los soldadores eléctricos. En la mayor parte de las oficinas esto no es un problema, otros aparatos de la oficina, como son las fotocopiadoras, están normalmente apantalladas. Sin embargo, los ascensores pueden ser un problema en los edificios de oficinas, y el uso industrial de las computadoras crece rápidamente. Por ello, en algunos casos será necesario encerrar la computadora personal en una caja metálica, para protegerla de las interferencias del ruido eléctrico.

- **Otros equipos informáticos**

  Un buen supresor de subidas de tensión y ruido, filtrará la interferencia por ruido en la red entre los distintos componentes conectados a él. Sin embargo la carcasa exterior de algunos componentes puede que no esté adecuadamente apantallada, dando lugar a interferencias entre los dispositivos. Es útil no olvidar que los problemas de incompatibilidad por ruido electromagnético aparecen de cuando en cuando, incluso con productos del mismo fabricante.

H. CONMUTACIÓN

Cuando se abren o cierran los conmutadores, algo de electricidad se escapa en forma de chispa, corto, sobretensión o pico. Si se conecta y desconecta un secador de pelo en una habitación oscura probablemente verá este fenómeno. Si desenchufa el secador mientras está funcionando probablemente verá una chispa en el enchufe.

Estas chispas pueden tener dos aspectos negativos sobre los sensibles equipos de las computadoras. En primer lugar el pico, la subida brusca de voltaje frente a la que nos protegen los protectores de picos.

El segundo efecto negativo de la conmutación es el tema mucho más complejo de los armónicos, frecuencias eléctricas sustancialmente más altas que la corriente que las ha producido.

La acción rápida del conmutador tiene el mismo efecto que el golpe con el dedo que produce armónicos en la cuerda de una guitarra. La generación de estas frecuencias no deseadas por un elemento del equipo, puede interferir con el funcionamiento de un elemento próximo.

Los buenos protectores ante sobretensiones y picos que suministran tensión a más de un elemento, ofrecerán algún tipo de aislamiento para cada elemento con el objetivo de evitar este problema, algunas veces descrito como ruido.

Reglas para evitar problemas de conmutación

Se puede ayudar a evitar estos problemas siguiendo las siguientes reglas:

- No enchufar ni desenchufar aparatos eléctricos que estén encendidos.
- No enchufar ni desenchufar especialmente las computadoras, impresoras y monitores. A menudo estos aparatos poseen alguna forma de protección en sus circuitos de conexión que no pueden actuar. Debido a que conectar por separado cada elemento del equipo puede ser una rutina desagradable, puede ser recomendable utilizar un centro de conexión, una unidad con protección

ante sobretensiones y picos con diseño en forma de consola que alimenta a todos los elementos del sistema.

I. SUMINISTRO ELECTRÓNICO

Las caídas, subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras, monitores, las impresoras y los demás periféricos.

Un corte de la alimentación de la unidad principal puede:

- Hacer que desaparezca la información que hay en la RAM. Los datos recién introducidos o recién editados que no se hayan grabado, se pierden.
- Se interrumpe el proceso de escritura en el disco. Se puede perder información de importancia que necesita el sistema operativo, como puede ser la localización de un archivo, dando como resultado que pierdan o desorganicen archivos.
- Puede "aterrizar" un disco fijo. La cabeza de lectura – escritura de la mayor parte de los discos fijos se separa automáticamente del disco cuando se desconecta la unidad, pero puede ocurrir en algunos sistemas que la cabeza "aterrice" sobre la superficie del disco y la dañe, dando lugar a que se pierdan datos e incluso, resulte dañado físicamente el disco.
- Interrumpir impresión. Cuando vuelva la tensión se han de continuar los procesos de impresión. En algunos casos se ha de volver a comenzar el proceso de impresión.
- Se interrumpen las comunicaciones. Cuando vuelve la corriente, los datos que se estaban transfiriendo entre las computadoras deben de ser comprobados para tener exactitud, y los archivos que se estaban transmitiendo puede que haya que volver a transmitirlos.
- Detiene el trabajo.
- El sistema queda expuesto a picos y subidas de tensión cuando vuelve la tensión. Normalmente se desconectan los equipos cuando se va a la corriente, pero esto no siempre es posible. Cuando la empresa de electricidad restaura el servicio, a menudo viene con picos que pueden dañar los aparatos que no se hubieran desconectado.

1. UPS o SAI (SISTEMA DE ENERGIA ININTERRUMPIBLE)

Energía de seguridad para un sistema de computación, cuando la energía eléctrica de la línea se interrumpe o baja a un nivel de tensión inaceptable. El UPS suministra electricidad a una PC (estación o servidor) cuando falla el fluido eléctrico. Esta unidad hace transparente a las interrupciones de fracciones de segundo que inevitablemente detiene a los sistemas y le permite seguir trabajando durante varios minutos. Los pequeños sistemas UPS proveen energía de baterías por sólo unos pocos minutos. Los sistemas más sofisticados están conectados a generadores eléctricos y pueden proveer energía durante días enteros. Los sistemas UPS proveen generalmente protección contra sobrecarga y pueden proveer asimismo regulación de tensión.

Selección de un UPS. Al seleccionar un UPS se debe tener en cuenta los siguientes factores principales:

- Requerimientos de Potencia (actuales y futuros)
- Requerimiento de frecuencia
- Tiempo de respaldo requerido
- Futuras Expansiones
- Picos por corriente de arranque
- Servicio de mantenimiento
- Soporte técnico (antes, durante y después de la instalación)

2. GRUPO ELECTRÓGENO

Son máquinas que generan energía eléctrica, aprovechando la energía máxima producida por máquinas de combustión interna.

Una planta generadora ideal, deberá tener el rendimiento y capacidad adecuada para alcanzar los requerimientos de carga que va a soportar. Esto hará que no tenga capacidad excesiva o funciones innecesarias que incrementarían el costo inicial y el costo de operación.

Para obtener el rendimiento y la confiabilidad adecuada, se debe declarar las especificaciones en términos de rendimiento deseado, en vez de intentar especificar un determinado tamaño, tipo o marca de equipo.

Es necesario mencionar que el circuito de generación eléctrica produce extraños voltajes y corrientes en el circuito de comunicación telefónica. Esto puede ser peligroso para las personas o puede dañar los aparatos o interferir las comunicaciones. Por eso, se debe evitar la proximidad de un grupo electrógeno con los circuitos telefónicos y proteger éstos con dispositivos que eviten los peligros y la interferencia.

Tablero de Control. El tablero de control debe ser diseñado de acuerdo al voltaje y corriente que se propone soportar, y debe ser equipado con los dispositivos necesarios de protección contra fallas para proteger al generador de daños, cuando hay fallas o sobrecargas en el sistema.

Mantenimiento

La limpieza con paño seco puede ser satisfactoria cuando los componentes son pequeños. Generalmente se debe soplar la suciedad con aire comprimido, especialmente en los lugares donde se ha juntado tierra y no se puede llegar con el paño.

El polvo y la tierra pueden quitarse con una escobilla de cerdas y luego aspirar. No usar escobilla de alambre.

Los componentes eléctricos, después de la limpieza, almacenamiento o embarque deben secarse antes de hacerlos funcionar.

Comprobar la zona alrededor de las aberturas de admisión y escape del aire estén limpias y sin obstrucciones.

Inspeccionar que no haya conexiones sueltas o contaminadas. Si durante la inspección se muestra que los revestimientos de barniz se han deteriorado, se les debe volver a cubrir con barniz de aislamiento.

Como regla general, los cojinetes deben lubricarse anualmente. Condiciones de operación muy severas, tales como ambientes muy calurosos y polvorientos, requerirán una lubricación más frecuente.

En caso que los grupos electrógenos sean usados sólo en emergencias, se debe establecer una política o procedimiento de puesta en funcionamiento para mantener operativo los equipos.

J. ACCIONES HOSTILES

1. ROBO

Los equipos de cómputo son posesiones muy valiosas de la MPB y están expuestas al "robo", de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen el computador de la institución en realizar trabajos privados para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraída, cintas y discos son fácilmente copiados sin dejar ningún rastro.

Cómo evitar el robo:

- Colocar plataformas de anclaje en los diferentes elementos del computador (monitor, cpu, impresora, etc.)
- Diseñar muebles para ordenadores de forma que se pueda asegurar fácilmente la máquina y los periféricos (Tapas con llave, puertas, etc.).
- Evitar que quiten la tapa del ordenador y se lleven la unidad y tarjetas adaptadoras.

Cómo prevenir los robos con computadora

- Adoptando un sistema operativo de última tecnología y que permita el acceso a los equipos de acuerdo a las funciones de cada usuario.
- Creación de un equipo con misión especial que establezca y compruebe técnicas de seguridad para la computadora. Este equipo deberá incluir representantes de los departamentos de procesamiento de datos, seguridad, auditoría y usuario.
- Ejecución de un análisis de riegos en los sistemas que abarquen pérdidas potenciales por accidentes, así como por delitos intencionados.
- Establecer inspecciones y entrevistas que abarquen:
    - Estado físico del local de la computadora y departamentos de usuarios.
    - Control de acceso.
    - Documentación
    - Segregación de deberes. Separar (Planeamiento/Desarrollo de Ejecución y de Verificación/Control)
    - Trabajo excesivo o innecesario del personal.
    - Entorno general personal.
    - Prestar atención especial a la información contable.

Evitar

- Depender de una sola persona para las funciones vitales.
- Repetición periódica de comprobaciones de seguridad. Emplear inspecciones ad-hoc
- Trabajo no supervisado, especialmente durante el turno de noche. Malas técnicas de contratación, evaluación y de despido de personal.

2. FRAUDE

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, los computadores han sido utilizados en dicho propósito.

En realidad, el potencial de pérdida a través de fraudes, y los problemas de prevención y detección del fraude, están en aumento en sistemas computarizados. Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.) tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones:

Las tres principales áreas donde se produce el fraude son:

a. Manipulación de información de entrada, fácil de realizar y muy difícil de detectar, al ser los métodos de validación de entrada simples y, en general, conocidos por un gran número de personas de la empresa.
b. Alteración o creación de archivos de información. Se alteran los datos directamente del fichero o se modifica algún programa para que realice la operación deseada.
c. Transmisión ilegal. Interceptar o transferir información de teleproceso.

Entornos que conducen al fraude con computadoras

- Baja moral entre el personal. Los colaboradores en los departamentos de procesamiento de datos y usuarios de la computadora, muestran falta de disciplina respecto a las precauciones de seguridad y en mantener una operación ordenada y sistemáticamente realizada.
- Documentación deficiente. La documentación del sistema está incompleta, anticuada y desordenada. Sólo el diseñador del sistema tiene una idea verdadera de lo que hace el sistema.
- Colaborador innecesariamente atareado por todo el tiempo. Colaboradores con pocos permisos para ausentarse, en la misma función, durante largo tiempo y rara vez toman vacaciones (Una vez que un fraude está en marcha, el delincuente necesita mantener continua vigilancia para evitar ser descubierto).
- Falta de segregación de deberes. Se permite a los programadores ingresar datos, el personal de operaciones interviene en programación, etc.
- Deficiente administración de la operación. Falta de control de documentos y de procedimientos de autorización, regulando cambios del sistema y alteraciones a los ficheros de datos. Falta general de control del sistema.
- Alta incidencia de equivocaciones de la computadora. Errores creados por un diseño deficiente del sistema hacen que el personal y gerentes acepten errores susceptibles de "inculpar a la computadora".

3. SABOTAJE

El peligro más temido por los centros de Procesamiento de Datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Los imanes son herramientas muy recurridas, aunque las cintas estén almacenadas en el interior de su funda de protección, una ligera pasada y la información

desaparecerá. Una habitación llena de cintas puede ser destruida en pocos minutos. Los centros de Procesamiento de Datos pueden ser destruidos sin entrar en ellos. Suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

La protección contra el sabotaje requiere:

- Una selección rigurosa de los colaboradores.
- Buena administración de los recursos humanos.
- Buenos controles administrativos.
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.
- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

El problema de la seguridad del computador debe ser tratado como un problema importante de dirección. Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que puedan ponerse en práctica los adecuados métodos de prevención.

Una mejora en la seguridad produce, a menudo, importantes beneficios secundarios. Por ejemplo, el cambio de metodología aplicada a determinadas operaciones conduce frecuentemente a una reducción del índice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existe un plan idóneo o una recomendación simple para resolver el problema de seguridad. Realmente no es una situación estática o un problema "puntual" sino que requiere un constante y continuo esfuerzo y dedicación.

Se menciona a continuación algunas medidas que se deben tener muy en cuenta para tratar de evitar las acciones hostiles:

- Ubicar los equipos en lugares más seguros en donde se prevea cualquier contingencia de este tipo.
- Mantener una lista de números telefónicos de las diferentes dependencias policiales a mano y en lugares donde se pueda hacer un llamado de emergencia.
- Siempre habrá de tomarse en cuenta las Políticas de Seguridad en caso como terrorismo y sabotaje. Son importantes la medida de ingreso de personas debidamente identificadas, marcación de zonas de acceso restringido, prevención para explosivo, etc.
- Tener una comprensión realista de cómo los magnetos (imanes) pueden dañar el almacenamiento magnético.
- Mantener adecuados archivos de reserva (backups)
- Identificar y establecer operaciones críticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
- Montar procedimientos para remitir registro de almacenamiento de archivos y recuperarlos.
- Usar rastros de auditoría o registro cronológico (logs) de transacción como medida de seguridad.

CAPTIULO VI

FALLAS GENERICAS FUNCIONALES DE LOS SISTEMAS

A. FALLAS COMUNES

Se han encontrado varias fallas comunes a muchos sistemas de computación. Estos incluyen:

1. **Autentificación**

   Llamamos autentificación a la comprobación de la identidad de una persona o de un objeto. En muchos sistemas, los usuarios no pueden determinar si el hardware y el software con que funcionan son los que se supone que deben ser. Esto hace fácil al intruso reemplazar un programa sin conocimiento del usuario. Un usuario puede inadvertidamente teclear una contraseña en un programa de entrada falso.

2. **Cifrado**

   La lista maestra de contraseñas debe ser almacenada, cifrada, lo que a menudo no se hace.

3. **Implementación**

   Un diseño bien pensando de un mecanismo de seguridad puede ser implementado de forma improcedente.

4. **Confianza implícita**

   Un problema corriente, una rutina supone que otra está funcionando bien cuando, de hecho, debería estar examinando detenidamente los parámetros suministrados por la otra.

5. **Compartimiento implícito**

   El sistema puede depositar inadvertidamente información importante del sistema, en un espacio de direcciones del usuario.

6. **Comunicación entre procesos**

   El intruso puede usar un mecanismo de SEND/RECEIVE para probar varias posibilidades. Por ejemplo el intruso puede pedir un recurso del sistema y suministrar una contraseña. La información devuelta puede indicar "contraseña correcta", confirmando la contraseña adivinada por el intruso

7. **Verificación de la legalidad**

   El sistema puede no estar realizando una validación suficiente de los parámetros del usuario.

8. **Desconexión de línea**

   En tiempos compartidos y en redes, cuando la línea se pierde (por cualquier razón), el sistema operativo debe inmediatamente dar de baja del sistema al usuario o colocar al usuario en un estado tal, que sea necesaria la reautorización para que el usuario obtenga de nuevo el control. Algunos sistemas permiten que un proceso "flote" después de una desconexión de línea. Un intruso puede llegar a obtener el control del proceso y usar cualquier recurso a los que tenga acceso el proceso.

9. **Descuido del operador**
   Un intruso puede engañar a un operador y hacer que cargue un paquete de disco con un sistema operativo falso.

10. **Paso de parámetros por referencia en función de su valor**
    Es más seguro pasar los parámetros directamente en registros, que tener los registros apuntando a las localidades que contienen los parámetros. El paso por referencia puede llevar a una situación en la cual los parámetros, pueden aún encontrarse en el espacio de direcciones del usuario después de una verificación de la legalidad. El usuario podría así suministrar parámetros legítimos, verificarlos, y modificarlos justo, antes de ser utilizados por el sistema.

11. **Contraseñas**
    Las contraseñas son, a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse con número máximo (3) de intentos infructuosos.

12. **Entrampamiento al intruso**
    Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

13. **Privilegio**
    En algunos sistemas hay demasiados programas con muchos privilegios. Estos es contrario al principio del menor privilegio.

14. **Confinamiento del programa**
    Un programa prestado de otro usuario puede actuar como caballo de Troya: puede robar o alterar los archivos del usuario que los prestó.

15. **Residuos**
    A menudo el intruso puede encontrar una lista de contraseñas con sólo buscar en una papelera. Los residuos se dejan a veces en el almacenamiento después de las operaciones rutinarias del sistema. La información delicada debe ser siempre destruida antes de liberar o descargar el medio que ocupa (almacenamiento, papel. Etc.). Las trituradoras de papel son algo corriente en ese aspecto.

16. **Blindaje**
    Una corriente en un cable genera un campo magnético alrededor de él, los intrusos pueden de hecho conectarse a una línea de transmisión o a un sistema de computación sin hacer contacto físico. Puede usarse el blindaje eléctrico para prevenir tales "intrusiones invisibles"

17. **Valores de umbral**
    Están diseñados para desanimar los intentos de entrada, por ejemplo. Después de cierto número de intentos inválidos de entrar al sistema, ese usuario (o el terminal desde donde se intentan las entradas) debe ser bloqueado y el administrador del sistema, advertido. Muchos sistemas carecen de esta característica.

B. ATAQUES GENÉRICOS A SISTEMAS OPERATIVOS

Ciertos métodos de penetración se han utilizado efectivamente en muchos sistemas.

1. **Asincronismo**
   Con procesos múltiples que progresan de forma asincrónica es posible que un proceso modifique los parámetros cuya validez ha sido probada por otro, pero que aún no ha utilizado. Con esto, un proceso puede pasar valores malos a otro, aun cuando el segundo realice una verificación extensa.

2. **Rastreo**
   Un usuario revisa el sistema de computación, intentando localizar información privilegiada.

3. **Entre líneas**
   Se usa un terminal especial para conectarse a la línea de comunicación mantenida por un usuario dado de alta en el sistema, que está inactivo en ese momento.

4. **Código clandestino**
   Se hace un parche en el sistema operativo bajo la pretensión de una depuración. El código contiene trampas que permite realizar a continuación reentradas no autorizadas al sistema.

5. **Prohibición de acceso**
   Un usuario escribe un programa para hacer caer al sistema, poner al sistema en un ciclo infinito, o monopolizar recursos del sistema. Lo que se intenta aquí es el negar el acceso o servicio a los usuarios legítimos.

6. **Procesos sincronizados interactivos**
   Los procesos usan las primitivas de sincronización del sistema para compartir y pasarse información entre sí.

7. **Desconexión de línea**
   El intruso intenta obtener acceso al trabajo de un usuario después de una desconexión de línea, pero antes de que el sistema reconozca la desconexión.

8. **Disfraz**
   El intruso asume la identidad de un usuario legítimo, después de haber obtenido la identificación apropiada por medios clandestinos.

9. **Engaño al operador**
   Un intruso asume la identidad de un usuario legítimo, después de haber obtenido la identificación apropiada por medios clandestinos.

10. **Parásito**
    El intruso utiliza un terminal para conectase a una línea de comunicación. El intruso intercepta los mensajes entre el usuario y el procesador, modifica el mensaje o lo reemplaza por completo.

11. Caballo de Troya

El intruso coloca un código dentro del sistema que le permita accesos posteriores no autorizados. El caballo de Troya puede dejarse permanentemente en el sistema o puede borrar todo rastro de sí mismo, después de la penetración.

12. Parámetros inesperados

El intruso suministra valores inesperados a una llamada al supervisor, para aprovechar una debilidad de los mecanismos de verificación de la legalidad del sistema.

A medida que la computación se hace más asequible, los problemas de seguridad aumentan. Las comunicaciones de datos y las redes suponen un gran aumento de la vulnerabilidad de los sistemas. El hecho de ser favorables al usuario, implica también un incremento de la vulnerabilidad.

La seguridad externa se ocupa de la protección del sistema de computación contra intrusos y desastres. La seguridad de la interface del usuario se encarga de establecer la identidad del usuario antes de permitir el acceso al sistema. La seguridad interna se encarga de asegurar una operación confiable y sin problemas del sistema de computación, y de garantizar la integridad de los programas y datos.

La autorización determina que acceso se permite a qué entidades. La división de responsabilidades da a la gente distintos conjuntos de responsabilidades. Ningún empleado trata con una gran parte de la operación del sistema, de modo que para comprometer la seguridad tienen que estar implicados varios empleados.

La vigilancia trata de la supervisión y auditoría del sistema, y de la autentificación de los usuarios. En la verificación de las amenazas, el sistema operativo controlar las operaciones delicadas, en vez de darle el control directo a los usuarios. Los programas de vigilancia realizan operaciones sensibles.

Cuando los programas de vigilancia han de tener un acceso mayor que los programas del usuario, para servir las peticiones del usuario, esto se denomina amplificación.

CAPITULO VII

SEGURIDAD EN REDES

A. PROBLEMAS BÁSICOS

En el intento de proteger una red de computadoras, existen varias funciones comunes a las cuales deben dirigirse. La siguiente es una lista de cuatro problemas básicos:

1. EL ANFITRION PROMISCUO

a. El anfitrión promiscuo es uno de los principales problemas de seguridad y uno de los problemas más urgentes de cualquier red.
b. Si un intruso es paciente, él puede simplemente mirar (con una red debugger o anfitrión promiscuo) que los paquetes fluyen de aquí para allá a través de la red. No toma mucha programación el análisis de la información que fluye sobre la red.
c. Un ejemplo simple es un procedimiento de login remoto. En el procedimiento login, el sistema pedirá y recibirá el nombre y contraseña del usuario a través de la red.

2. AUTENTICACIÓN

a. El procedimiento de login remoto ilustra el problema de autenticación. ¿Cómo se presenta al anfitrión remoto para probar que usted es usted?
b. ¿Cómo se hace esto, de forma que no se repita el mecanismo simple de una jornada registrada?

3. AUTORIZACIÓN

Aun cuando se probar que usted es quien dice ser, simplemente, ¿Qué información debería permitir el sistema local acceder a través de una red?. Este problema de autorización parecería ser simple en concepto, pero considerar los problemas de control de acceso, cuando todo el sistema tiene su identidad remota de usuario, el problema de autorización sería un problema de seguridad bastante serio, en donde intervienen los conceptos de funciones autorizadas, niveles de autorización, etc.

4. CONTABILIDAD

a. Finalmente, considerar el problema de contabilidad. Hay que recordar que nosotros debemos asumir que hay otros con un conocimiento mayor de sistemas.
b. ¿Cuánta contabilidad tiene que hacer el sistema de crear una pista de revisión y luego examinar?

B. COMPONENTES DE SEGURIDAD

Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla. El administrador de la red tal vez que tenga que clasificar a los usuarios de la red con el objeto de adjudicarles el nivel de seguridad adecuado. A continuación se detallan sistema en tres niveles:

1. Nivel de administración

Aquellos que diseñan, mantienen o ponen en marcha la red. Este debe estar constituido sólo por el administrador o por un pequeño grupo de personal de soporte y administración.

2. **Usuarios fiables**
   Aquellos usuarios que cumplen las normas y cuyo trabajo se puedan beneficiar de una mayor libertad de acceso a la red.

3. **Usuarios vulnerables**
   Aquello que muestran falta de competencia, son excesivamente curiosos o beligerantes, o los que por alguna razón no se puede confiar.

Estos niveles pueden tener un reflejo en el número de barreras que se establecen para el acceso al sistema y el tipo de derechos de acceso que se conceden, para cuando se ha obtenido la conexión, así como el nivel de supervisión y la frecuencia de las comprobaciones.

C. CONTROL DE ACCESO A LA RED

1. Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y/o sistemas biométricos.
2. Restringir la posibilidad de conectar estaciones mediantes llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
3. Identificación para la red con clave de acceso.
4. Proteger con clave de todas las áreas sensitivas de datos y restricción de acceso a los programas, según su uso.
5. Registrar toda la actividad de la estación de trabajo.
6. Proteger con clave de acceso o bloqueo de todas las operaciones de copia a disquete en las estaciones de trabajo.
7. Monitorizar todas las operaciones de copia en disquete en las estaciones de trabajo.

D. PROTECCION DEL SERVIDOR

La parte más importante de la red es el servidor. La concentración de los datos en el servidor, en términos de cantidad e importancia, hace que sea necesario protegerlo de todas las eventualidades.

La dependencia en que esté el servidor no debe ser accesible para nadie, excepto para el administrador de la red. No se debe permitir que personas que no han de utilizar el servidor estén cerca de él. Las impresoras y otros periféricos deben mantenerse alejados de ojos fisgones.

Dada la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia otro local).

E. REDES Y TOLERANCIA A FALLAS

La tolerancia a fallas es la capacidad de la red de continuar funcionando, en el caso que se produzca un problema importante o una caída catastrófica, sin daño para los datos y sin que el funcionamiento cambie perceptiblemente.

Tolerancia a Fallas (TF) en una red significa que si ocurre una falla en uno de sus componentes, esta continuará funcionando, y se logra aplicando un conjunto de disposiciones que se explicarán posteriormente y deben ser aplicados a cada uno de los componentes de la red.

Las redes son Flexibles a Fallas, cuando al ocurrir alguna, esta deja de funcionar, pero al sustituir el componente afectado se restaura el servicio en un corto tiempo.

La tolerancia a fallas, se refiere no sólo a la redundancia, sino a la detección de errores. Por lo general, la tolerancia a fallas conduce a un elemento hardware redundante, que entra en funcionamiento de forma automática en el caso que el componente primario falle. Sin embargo la tolerancia a fallas puede ser algo como duplicar la FAT (tabla de localización de archivos) y las entradas de directorio en áreas distintas de un mismo disco, o una simple verificación de lectura tras escritura, con lo que se asegura que los datos nunca se escriben en un sector dañado del disco.

No todas las redes requieren el mismo grado de tolerancia a fallas.

Acciones para tener en cuenta:

- Disponer de UPS para todas las computadoras que considere críticas para la MPB.
- Instale doble tarjeta de interfaz a la red en cada una de la computadoras y conectarlas en segmentos separados de la red.
- No se debe desestimar lo obvio, un ratón o un teclado se pueden dañar y generar inconvenientes innecesarios. Se debe tener un Kit de componentes de las computadoras en stock.
- No se debe utilizar el disquete como medio de respaldo, hay que emplear esquemas reales de respaldo. Realice el respaldo y verifíquelo. Certifique éstos respaldos. Analice los Logs con los resultados de los respaldos.

F. LAS ESTACIONES DE TRABAJO SIN FLOPPY DISK

Una posible solución para poder impedir la copia de programas y datos fuera de la red en disquetes, y que a través de los disquetes ingresen virus y otros programas dañinos a la red, es dotar a los usuarios vulnerables con estaciones de trabajo sin floppy disk.

CAPITULO VIII

IMPLEMENTACION

Para este caso se tiene que tener preparado los planes de contingencia para poder aplicarlos. Puede también tratarse esta etapa como una prueba controlada.

A. EMERGENCIA FÍSICAS (CASOS)

1. Error Físico de Disco de un Servidor (Sin RAID)

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

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

2. Error de Memoria RAM

En este caso se dan los siguientes síntomas:

a. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
b. Ante procesos mayores se congela el proceso.
c. Arroja errores con mapas de direcciones hexadecimales
d. El servidor contará con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.
e. Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie cambiarlo.
f. Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:
    - 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.

3. **Error de Tarjeta(s) Controladora(s) de Disco**

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

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

4. **Caso de incendio Total**

La mejor manera de prevenir un incendio es no provocarlo. Observe las prohibiciones de no fumar y las normas de prevención propias del local en que se encuentre, y con mayor razón en un centro de cómputo.

<u>En presencia del fuego tenga en cuenta que:</u>

- Puede tratar de apagar un fuego en una oficina siempre que tenga detrás una puerta que le permita salida.
- Si el fuego prende en sus ropas, no corra, tírese al suelo y ruede. Si el hecho ocurre a otra persona cúbrala con alguna prenda o con una toalla humedecida, si se encuentra próximo a un aseo. No se quite la ropa si tiene quemaduras.
- En presencia de aparatos eléctricos, no eche agua al fuego. Tampoco debe hacerlo ante líquidos inflamables (alcohol, aceite, gasolina, etc.).
- Si hay mucho humo póngase un pañuelo en la boca y nariz, a ser posible mojado, y salga agachado o gateando. Respire profundamente para evitar desvanecimientos.
- Al salir de una dependencia, procure cerrar las ventanas y las puertas, pues las corrientes avivan el fuego.
- Si se encuentra aislado y no puede ponerse a salvo, diríjase a la habitación más alejada del fuego (pero no a un nivel superior a menos que esté seguro de que los equipos de rescate se encuentran muy cerca y provistos de escaleras largas u otro equipo.
- Si se ve obligado a huir a través de las llamas para ponerse a salvo, no se entretenga en recoger nada, cúbrase (incluyendo la cabeza) con una manta, una toalla, una cortina o un abrigo mojado si es posible, luego aguante la respiración y corra.

<u>Con respecto a los equipos de cómputo</u>

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 se tuviera.

a. Ante todo, se debe conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, se debe tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
b. 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).
c. Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas.
d. 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 posible, por las salidas destinadas para ello.

5. Caso de Inundación

a. 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.
b. En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
c. 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.
d. Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.
e. Proveer cubiertas protectoras para cuando el equipo esté apagado.

6. Caso de Fallas de Fluido Eléctrico

Se puede presentar lo siguiente:

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

Llámese corriente de emergencia a la brindada por grupo electrógeno y/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)

CAPITULO IX

MEDIDAS DE PRECAUCION

A. EN RELACION AL CENTRO DE COMPUTO

a. Los equipos no deben estar ubicados en las áreas de alto tráfico de personas o con un alto número de invitados.
b. Con respecto a los grandes ventanales, se deben cubrir con persianas, cortinas o algún protector para evitar la entrada de sol y calos, los cuales son inconvenientes para el equipo de cómputo, puede ser un riesgo para la seguridad de los mismos.
c. Otra precaución que se debe tener en el cuidado de los equipos es que en la oficina no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no queden perfectamente selladas y despidan polvo.
d. 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.
e. Al momento de reclutar a los nuevos colaboradores se les debe realizar exámenes psicológicos y médico, y tener muy en cuenta sus antecedentes de trabajo en otras instituciones, ya que un Centro de Cómputo depende en gran medida, de la integridad, estabilidad y lealtad de los colaboradores.
f. El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.
g. Establecer 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.
h. Establecer políticas para la creación de los password y establecer periodicidad de cambios de los mismos.
i. Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.
j. Establecer políticas de control de entrada y salida del personal, así como de los paquetes y objetos que portan.
k. La seguridad de las terminales de un sistema en red deben de 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 informático.
l. 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.
m. Las cámaras fotográficas no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la Unidad.
n. Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

B. RESPECTO A LA ADMINISTRACIÓN DE LOS BACKUPS

a. Se administrará bajo la lógica de un almacén, esto implica ingreso y salida de medios magnéticos (cintas, disquetes, cartuchos, discos removibles, CD's, etc.) obviamente teniendo más cuidado con las salidas y cuidando que el grado de temperatura y humedad sean los adecuados.

b. Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.
c. El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.
d. El proceso de etiquetado tiene que estar registrado.

C. RESPECTO A LA ADMINISTRACIÓN DE IMPRESORAS

a. Todo listado que especialmente contenga información confidencial, debe ser destruido.
b. Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.
c. Establecer controles respecto a los procesos remotos de impresión.

D. PARA EL MANTENIMIENTO DE LOS DISCOS DUROS

a. Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.
b. El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.
c. Evitar que la microcomputadora se coloque en zonas donde haya acumulación de calor. Ésta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.
d. No mover el CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.
e. Para mantener la velocidad en el equipo, se debe realizar una vez al mes el proceso de desfragmentación para conservar en óptimo estado la respuesta del equipo.
f. Una de las medidas más importantes en este aspecto, es hacer que la gente toma conciencia de lo importante que es cuidar un microcomputador.

E. RESPECTO A LOS MONITORES

a. Usar medidas contra la refección para reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día.
b. Sentarse por lo menos a 60 cm de la pantalla. No sólo esto reducirá su exposición a las emisiones (que se disipan a una razón proporcional al cuadrado de la distancia), sino que puede ayudar a reducir el esfuerzo visual.
c. También manténgase por lo menos a 1m o 1.20m del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.
d. Finalmente apague su monitor cuando no lo esté usando

F. PARA EL CUIDADO DEL EQUIPO DE CÓMPUTO

a. Teclado. Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función. Para eliminar el polvo del teclado, lo más conveniente es voltearlo y soplar el aire comprimido para que éste salga completamente. Se debe evitar en lo posible quitar las tapas de las teclas de la PC para lavarlas, ya que su reposición puede generar fallas mecánicas.
b. CPU. Mantener la parte posterior del cpu liberado en por lo menos 10cm. Para asegurarse así una ventilación mínima adecuada.

c. Mouse. Poner debajo del mouse una superficie plana y limpia, a fin de mantener el buen funcionamiento de éste.
d. Caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado.
e. Papelera de reciclaje. Windows reserva un 10 por ciento de la capacidad del disco duro para mantener algo de la información que ya se haya eliminado, con la finalidad de que en cualquier momento se pueda recuperar. No obstante, la papelera de reciclaje, ubicada en el Escritorio de la computadora, debe limpiarse con regularidad para no llenarse de basura que le estará quitando espacio en disco duro.
f. Término de sesión o apagado. En muchas ocasiones, por la prisa o mal uso de la computadora, no se cierran las aplicaciones correctamente o bien, no se apaga la computadora de forma adecuada, esto provoca pérdida de información y daña el sistema operativo.

DISPOSICIONES FINALES

1. El Plan de Contingencias contará con el apoyo correspondiente por parte de la Alta Dirección, para suministrar recursos financieros, humanos y materiales a fin de su implementación y ejecución.
2. Realizar la conformación de un Comité Técnico Institucional, el cual sea el encargado de planificar, implementar y supervisar la ejecución del Plan de Contingencias Informático, que asegure la legalidad, consistencia, adecuado uso, seguridad, inviolabilidad y sostenibilidad de los Sistemas de Información, hardware y software.
3. Los Gerentes, SubGerentes, Jefes y colaboradores que laboren en la Municipalidad Provincial de Barranca, deben tomar parte de las actividades y están obligados a participar de la implementación y ejecución del Plan de Contingencias.
4. Definir políticas de seguridad, como una herramienta para el control permanente del cumplimiento del Plan de Contingencias.
5. Las medidas que debemos adoptar para protegernos son tantas como amenazas existen, es por ello que se debe difundir a todas las áreas de la Municipalidad copias del Plan, documentos resumen, carteles, afiches y otro tipo de documento para su información.
6. Realizar las acciones necesarias para cumplir y hacer cumplir los objetivos y funciones determinadas en el presente Plan de Contingencias, y así cumplir con las disposiciones legales vigentes dispuestas por al ONGEI