POLITICAS DE MITIGACION DE RIESGOS

TOMO I

PLANES DE CONTINGENCIA

Gabriela A. Castaño

2001

INDICE GENERAL

TOMO I - *PLANES DE CONTINGENCIAS*

RESUMEN EJECUTIVO III

VALOR AGREGADO V

ACTIVIDAD 1 - REQUISITOS MÍNIMOS PARA LA ELABORACIÓN DE PLANES DE CONTINGENCIA 1

ACTIVIDAD 2 - ESTUDIO Y ANÁLISIS DE LAS NORMAS Y REGLAMENTACIONES 33

ACTIVIDAD 3 – ELABORACIÓN DE PLANES DE CONTINGENCIAS PARA HARDWARE Y SOFTWARE 66

ACTIVIDAD 4 - CONCIENTIZACIÓN Y CAPACITACIÓN EN PLANES DE CONTINGENCIA 82

ANEXO I – Act. N°1 – 115

ANEXO II – Act. N°1 – 127

ANEXO III – Act. N°2 – 138

TOMO II - *PREVENCIÓN Y POLÍTICAS DE SEGURIDAD*

ACTIVIDAD 5 - MANUAL PARA EL BUEN USO DE LAS HERRAMIENTAS INFORMÁTICAS PARA EL USUARIO FINAL 1

ACTIVIDAD 6 - POLÍTICAS DE SEGURIDAD DE ALCANCE GENERAL 2

ACTIVIDAD 7 - PAUTAS GENERALES PARA LA CAPACITACIÓN Y CONCIENTIZACIÓN 36

ANEXO I – Act. N°6 – 69

ANEXO II – Act. N°6 – 78

ANEXO III – Act. N°6 – 85

ANEXO IV – Act. N°7 – 88

ANEXO V – Act. N°7 – 105

ANEXO VI – Act. N°7 – 112

ANEXO VII – Act. N°7 – 118

TOMO III – *MESA DE AYUDA*

ACTIVIDAD ADICIONAL - ASESORÍA EN EL PROCESO DE DESARROLLO DEL APLICATIVO Y MODELO DE TESTING 1

ACTIVIDAD 8 - DESARROLLO, IMPLEMENTACIÓN Y CAPACITACIÓN DEL SISTEMA DE MESA DE AYUDA - PRUEBA PILOTO 49

ACTIVIDAD 9 - ANÁLISIS Y EVALUACIÓN DEL SISTEMA DE MESA DE AYUDA 77

ACTIVIDAD 10 - ESTANDARES PARA USO Y FOMENTO DE LA HERRAMIENTA DE MESA DE AYUDA 110

ACTIVIDAD 11 - METODOLOGÍA DE REUTILIZACIÓN DE LA INFORMACIÓN 144

ANEXO I – Act. Adicional – 171

ANEXO II – Act. Adicional – 177

ANEXO III – Act. N°8 – 189

ANEXO IV – Act. N°9 – 208

RESUMEN EJECUTIVO

Fue nuestro objetivo principal dotar a la Intranet de gobierno de una serie de políticas para lograr minimizar los riesgos existentes en la actualidad en el ámbito informático.

Para ello previmos tres pilares fundamentales Sobre los cuales trabajar: Contingencias, Seguridad y Mesa de Ayuda, como herramienta básica para lograr el mínimo nivel de riesgo en la Intranet de Gobierno.

Planes de Contingencia: Se realizaron los requisitos mínimos indispensables para poder elaborar un plan de contingencia. Se generaron los planes de contingencia para hardware y software existentes al día dela fecha en la Secretaría de Estado de Tecnología de la Información (SETI). Por último se preparó un seminario para capacitar y concientizar a Usuarios Finales, Personal Jerárquico y Referentes Informáticos en el uso de los planes y las formas de prevenir las contingencias. Previa la generación de los mismos se realizó un estudio de las leyes nacionales y provinciales vigentes.

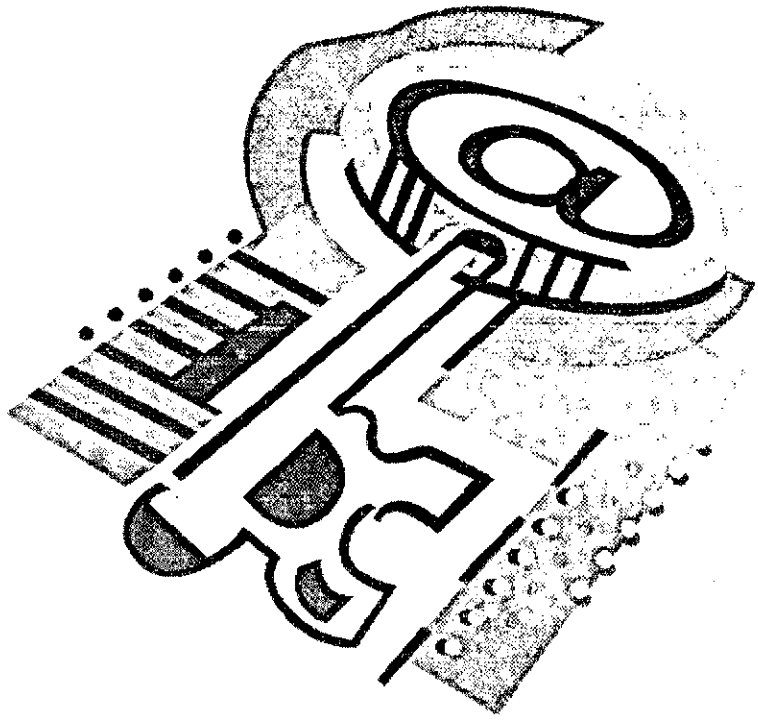
Prevención y Políticas de Seguridad: Se preparó un Manual para el Usuario Final en el uso y cuidado preventivo de las herramientas del hardware y software. Se definieron las políticas de seguridad de alcance general aplicables a toda la Intranet de Gobierno. Se crearon las pautas generales para las campañas de capacitación y concientización (por ejemplo: seminarios y cursos).

En ambos pilares se realizaron trabajos conjuntos con las áreas de redes, servidores, bases de datos, hardware y aplicativos.

Mesa de Ayuda: Se realizó la asesoría a la SETI para el desarrollo del aplicativo, realizado a medida. Se generaron los modelos de testing y prueba piloto orientados a esta herramienta. Se implementó el sistema y se desarrolló el modelo de auditoria. Por

último se creó la Metodología para mantenimiento y actualización de la Base y Librería de conocimiento de la Mesa de Ayuda.

Tanto el modelo de testing, como los de prueba piloto y auditoria pueden ser usados en forma general para cualquier otro aplicativo desarrollado a medida para la SETI de la Provincia de San Luis.



VALOR AGREGADO

Queriendo acompañar todo el proceso de modernización tanto del Estado provincial como del Consejo Federal de Inversiones y con la tendencia mundial de utilizar la Web como medio de publicación de información, hemos desarrollado y hacemos entrega con este Informe Final de la página web que contiene todas las actividades relevantes que se han desarrollado durante el desarrollo de este contrato. La misma ha sido diseñada con Front Page 2000 y puede ser accedida desde cualquier navegador.

El manual que ha sido realizado para el Usuario Final la Gerencia de Concientización Comunitaria ha decidido publicarlo y entregarlo dentro del ámbito de la Intranet Gubernamental.

Las campañas realizadas como parte de las medidas de Seguridad y Prevención (backup, antivirus, software legal, etc.) están siendo utilizadas por las diferentes Gerencias para llegar a los usuarios finales y Referentes informáticos.

El seminario de Concientización y Capacitación en planes de contingencia y seguridad está próximo a ser publicado en la Librería del conocimiento y a ser dictado por la Gerencia de Concientización comunitaria.

Además se hayan publicados en la Librería el Manual del Usuario Final y los instructivos para atención al publico de la Mesa de Ayuda.

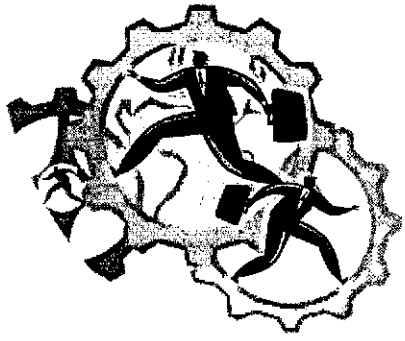
El aplicativo de la Mesa de Ayuda, como Help Desk y medida preventiva general ante los riesgos y contingencias posibles, se encuentra funcionando y abarca toda la Intranet de Gobierno.

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

ELABORACIÓN DE PLANES DE CONTINGENCIA



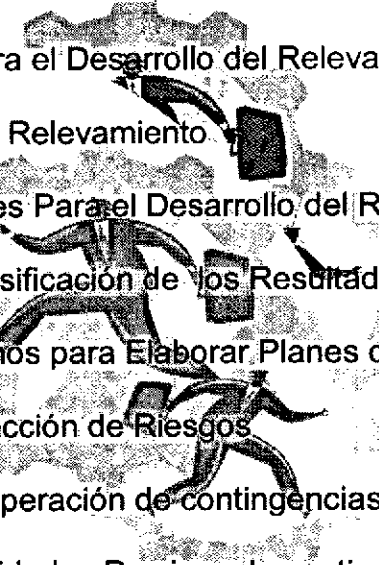
ACTIVIDAD 1

"REQUISITOS MÍNIMOS PARA LA ELABORACIÓN DE PLANES DE CONTINGENCIA"

"REQUISITOS MINIMOS PARA LA ELABORACIÓN DE PLANES DE CONTINGENCIAS"

Índice

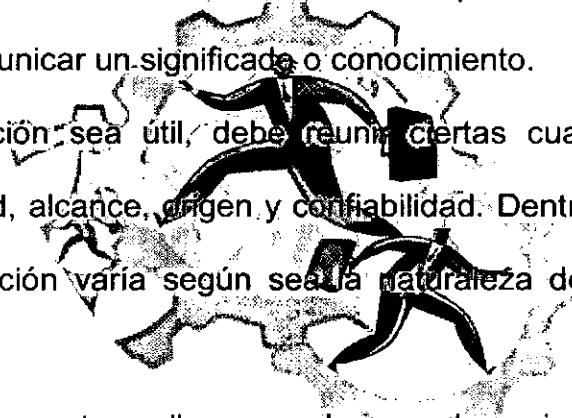
1. Enunciado
2. Objetivos
3. Cuerpo
    3.1. Relevamiento
        3.1.1. Desarrollo del Relevamiento
            a) Bases para el Desarrollo del Relevamiento
            b) Metas del Relevamiento
            c) Actividades Para el Desarrollo del Relevamiento
        3.1.2. Análisis y Clasificación de los Resultados
    3.2. Requerimientos Mínimos para Elaborar Planes de Contingencias
        3.2.1. Plan de Reducción de Riesgos
        3.2.2. Plan de Recuperación de contingencias
            3.2.2.1. Actividades Previas a la contingencia
            3.2.2.2. Actividades Durante la contingencia
            3.2.2.3. Actividades Después de la contingencia
4. Recomendaciones
5. Bibliografía



1. ENUNCIADO

La generación de los planes de contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos informáticos y la información contenida en los diversos medios de almacenamiento, es en definitiva, saber cómo reducir la posibilidad de ocurrencia y los procedimientos a seguir en caso que se presente un problema.

La información es uno de los principales recursos con los que cuentan las Organizaciones para la toma de decisiones, la planificación, la administración y el control. La base de toda información son los datos que se convierten en información con el objetivo de comunicar un significado o conocimiento.



Para que la información sea útil, debe reunir ciertas cualidades como exactitud, oportunidad, integridad, alcance, origen y confiabilidad. Dentro de una organización la necesidad de información varía según sea la naturaleza del trabajo y los objetivos buscados.

Es por ello que nuestra meta es llevar a cabo un relevamiento para determinar , por medio de la información recopilada u obtenida, la manera de generar un plan global y estándar que puedan utilizar las distintas Reparticiones del Gobierno de la Provincia de San Luis como guía para generar sus propios planes de contingencias.

2. OBJETIVO

Elaborar y definir los requisitos mínimos necesarios para la generación de los planes de contingencias que mejor se adecuen a la situación actual del estado, mediante la ejecución de un relevamiento de planes de contingencia existente dentro de la AAP (tanto en sistemas propios como tercerizados) y de un grupo de organizaciones privadas relevantes, tanto a nivel nacional como internacional.

Para poder elaborar los planes de contingencias se deben generar los requisitos mínimos que los mismos deberán cumplir, tanto los que se realizarán en este proyecto a nivel gerencial, como aquellos muy específicos que se generarán en las áreas técnicas como redes, servidores o base de datos. Se generará un estándar para la elaboración de los mismos para ser publicada y utilizada por toda la Intranet de gobierno.

El relevamiento contempla empresas que están actualmente trabajando para el gobierno de la provincia como Siemens, Tirón, Medifox y áreas internas con sistemas grandes como DOSEP.

En cuanto a empresas privadas externas: YPF (OPESSA), ORACLE, Ernest & Young Consulting, DGI, Telefónica Argentina S.A.

3. CUERPO

3.1. Relevamiento

3.1.1. Desarrollo del Relevamiento

Antes de comenzar a desarrollar este punto, es importante mencionar que las siguientes actividades fueron utilizadas, aplicadas y adaptadas de la Actividad N°9 del Proyecto Redes "**Relevamiento Integral Del Funcionamiento Del Estado Provincial En El Manejo De La Información**", en un todo de acuerdo con la autoría del mismo.

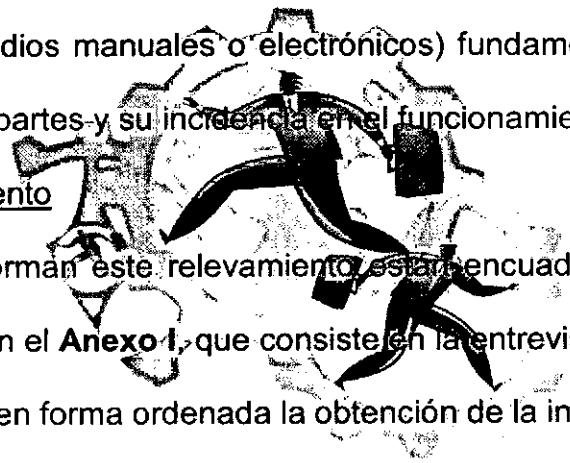
a) Bases para el Desarrollo del Relevamiento:

- La importancia significativa de contar con datos verídicos, motivo por el cual los relevamientos están dirigidos a personas involucradas y con conocimiento de causa de cada una de las áreas relevadas.

- La necesidad de conocer en profundidad el análisis de reducción de riesgos, como reducir la posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

- La necesidad de conocer la frecuencia de los movimientos de la información (cantidad de movimientos diarios, semanales, mensuales y anuales) y cuales son las políticas que existen para su seguridad y la del entorno de trabajo.

- Lograr obtener una visión real y clasificación de los movimientos del área relevada, como así también los medios por los cuales se traslada la información actualmente (medios manuales o electrónicos) fundamentales y secundarios, de cada una de las partes y su incidencia en el funcionamiento de la misma.



b) Metas del relevamiento

Las metas que conforman este relevamiento están encuadradas en la técnica de la entrevista, descripta en el **Anexo I**, que consiste en la entrevista de persona a persona, pudiendo planificarse en forma ordenada la obtención de la información necesaria, pero cabe aclarar que para algunos casos, también se utilizo la técnica de entrevistas por Correo Electrónico. Esto cumplimentaría los puntos mencionados en el informe anterior de Avance de esta misma actividad. (Pág. 3)

c) Actividades para el desarrollo del Relevamiento

El proceso de relevamiento, fue dividido en diversas etapas las que, una vez efectuadas, garantizarán el éxito de un relevamiento integral de las Organizaciones relevadas, siendo las mismas:

Definiciones a priori

- Definición de temáticas a relevar; esta actividad dio origen a las Bases para el desarrollo del Relevamiento, enunciadas en el apartado anterior.

- Definición del modelo de relevamiento.
- Cuando los datos provienen de las actitudes y/o las percepciones de los individuos, el método más directo para obtenerlos es la pregunta a estos mismos individuos. La observación nos sirve para obtener datos sobre el pasado o para determinar expectativas o intenciones respecto del futuro.

Limitaciones y riesgos

Es oportuno destacar que la entrevista tiene sus limitaciones y riesgos, de los cuales se fijaron políticas concretas de mitigación de los mismos. Podemos citar por ejemplo:

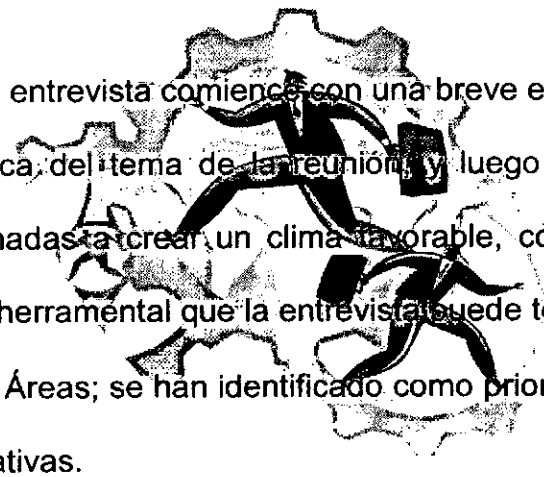
- Existen casos donde los datos que se pretenden obtener pueden afectar la situación del entrevistado o éste puede entender que ocurrirá tal afectación. Ante esta posibilidad, la táctica asumida es suponer que siempre existe esta afectación y tratar de superar este inconveniente con técnicas apropiadas.
- Debe considerarse que existe una tendencia natural a disimular cualquier posible falta de conocimiento. Ante esta situación, se ve la necesidad de verificar la garantía que ofrece el conocimiento del entrevistado, sin evidenciar esta actitud, ya que si fuese percibida por éste se produciría un refuerzo de la actitud defensiva que interrumpirá la comunicación.
- La flexibilidad y rapidez mental deben usarse siempre, pero basar el éxito de la entrevista en ellas es una prueba de falta de madurez y responsabilidad profesional. Los entrevistadores más experimentados no olvidan dedicar un tiempo prudente al planeamiento de cada entrevista.

Planeamiento

En el planeamiento se contempló:

- La definición clara y completa de los propósitos de la entrevista.

- La definición del porqué se elige al sujeto para la entrevista.
- Qué preguntas habrán de plantearse y cómo se las presentará.
- Como estructurar las preguntas para facilitar el recuerdo e intentar algún control de consistencia y para lograr que el entrevistado comprenda el mensaje.
- La definición de los elementos que se usarán para motivar al sujeto.
- La búsqueda de información para tomar conocimiento acerca de la personalidad de quien se va a entrevistar, para orientar la comunicación.
- La efectividad de la entrevista que varía en función del interés que el entrevistador pueda suscitar.
- Se definió que la entrevista comience con una breve explicación, no académica, ni doctrinaria, acerca del tema de la reunión, y luego continúe por una serie de preguntas destinadas a crear un clima favorable, convenciendo al entrevistado sobre la utilidad herramental que la entrevista puede tener respecto de sus fines.
- Identificación de Áreas; se han identificado como prioritarias las áreas de decisión y luego las operativas.
- Planeamiento estratégico del cronograma, para el desarrollo de las entrevistas.
- Concluida la entrevista se ofrece al entrevistado el resultado obtenido del relevamiento realizado.



Modelo de Entrevista utilizado

De las entrevista realizadas se utilizaron distintos modelos orientados a las dos áreas a relevar, tanto públicas como privadas, en los cuales se implementaron según el caso cuestionarios complementarios con el fin de profundizar en el tema. En las áreas privadas estos los mismos fueron acompañados por una Nota Presentación y aval de la

Secretaria de Estado de Tecnologías que podemos observar en el **Anexo II**: **Modelos de Cuestionarios.**

Formulación de entrevistas

Una vez definidas las normas practicas se debe establecer el planteo de la entrevista atendiendo a:

✓Lenguaje: preciso y usual para el entrevistado.

✓Ámbito: debe usarse el marco de referencia del entrevistado y adecuar la pregunta a su nivel de información.

✓Respuestas: no debe pedirse ninguna que sea inaceptable para el entrevistado, ni estar sugerida en las preguntas.

✓ Orden: debe facilitar el recuerdo yendo de lo general a lo particular.

3.1.2. Análisis y Clasificación de los resultados

De los datos obtenidos, los resultados son claros, debido a la falta de conocimiento de los entrevistados en temas de seguridad y planes de contingencias.

Podemos decir, que en las Áreas Publicas Provinciales (de ahora en mas APP) relevadas, estas medidas son escasas, teniendo en cuenta que para la mayoría de los entrevistados, el tema era desconocido y con una importancia menor, de lo que verdaderamente representa. Los resultados también nos muestran que las medidas de seguridad en sistemas en la totalidad de las APP, no cumplen con los requisitos mínimos como; copias de seguridad (backups), salidas de emergencia, normativas de trabajo, etc.

Mientras que en las áreas privadas, se cuenta con la documentación de planes de contingencias y seguridad previstos, pero en varios casos no son usados o aplicados, porque el personal no esta informado de su existencia y en aquellos casos en que si se

aplican, nos encontramos que en algunas situaciones, no están debidamente adaptados o actualizados.

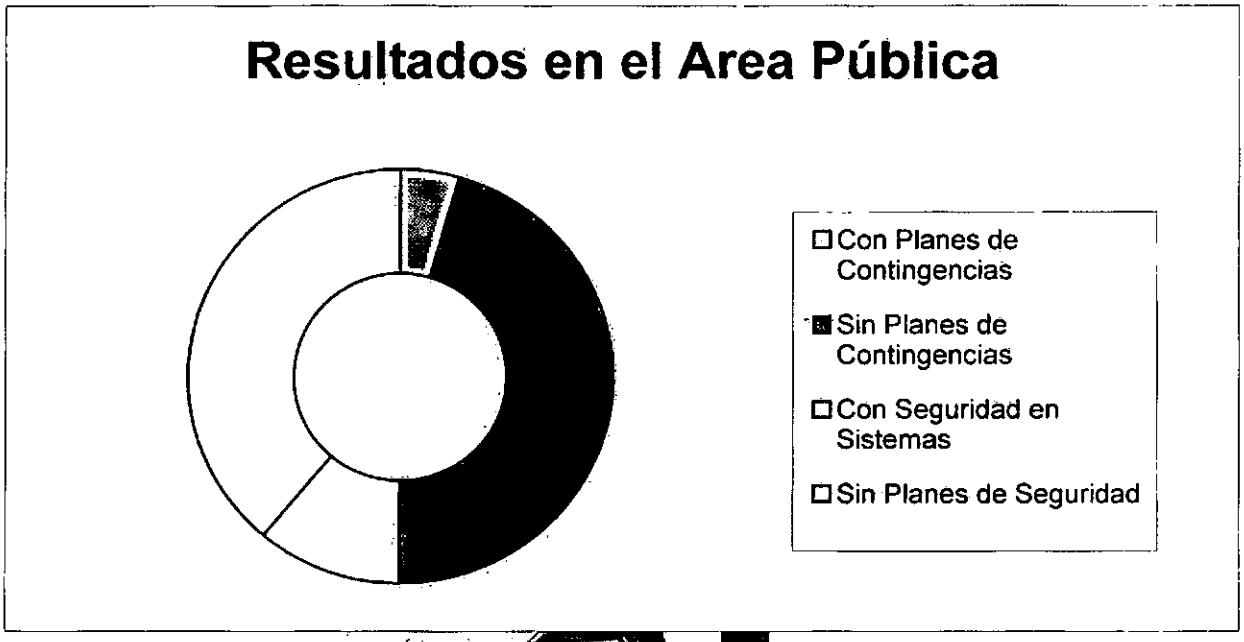


Figura N°1

Podemos observar en la **Figura N°1** que la APP, poseen un alto grado de Reparticiones que no tienen planes de contingencias o no realizan actividades de resguardo y seguridad.

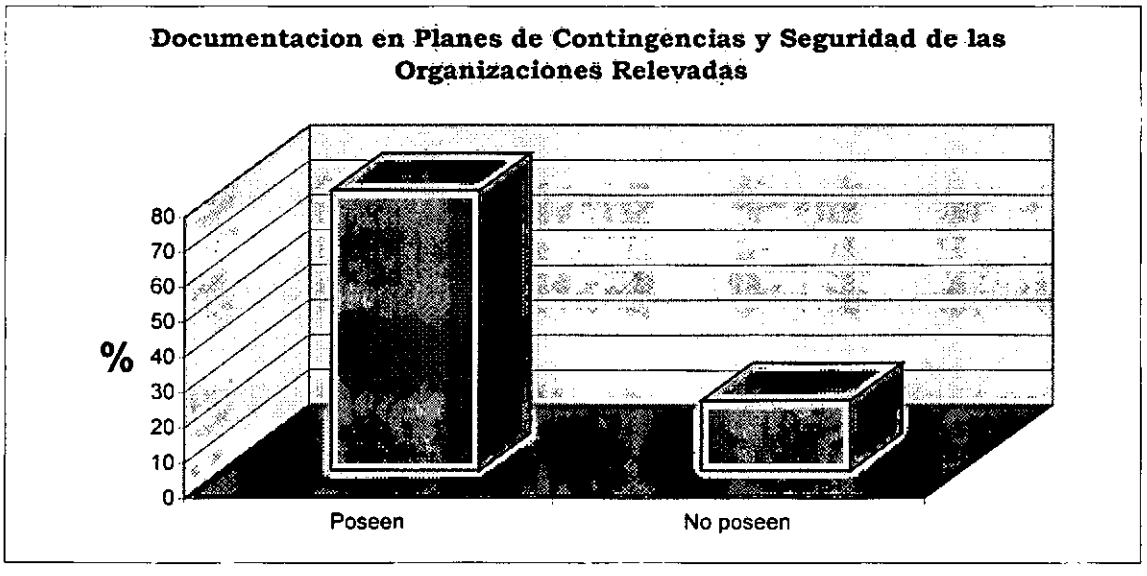


Figura N°2

En la **figura N° 2** el 80% de estas empresas del ámbito privado que han sido relevadas si están provistas de Planes de Seguridad y Contingencias, mientras que el 20% no poseen un estudio de estos, pero si de procedimientos aislados, que no son óptimos para una buena administración en la prevención de riesgos.

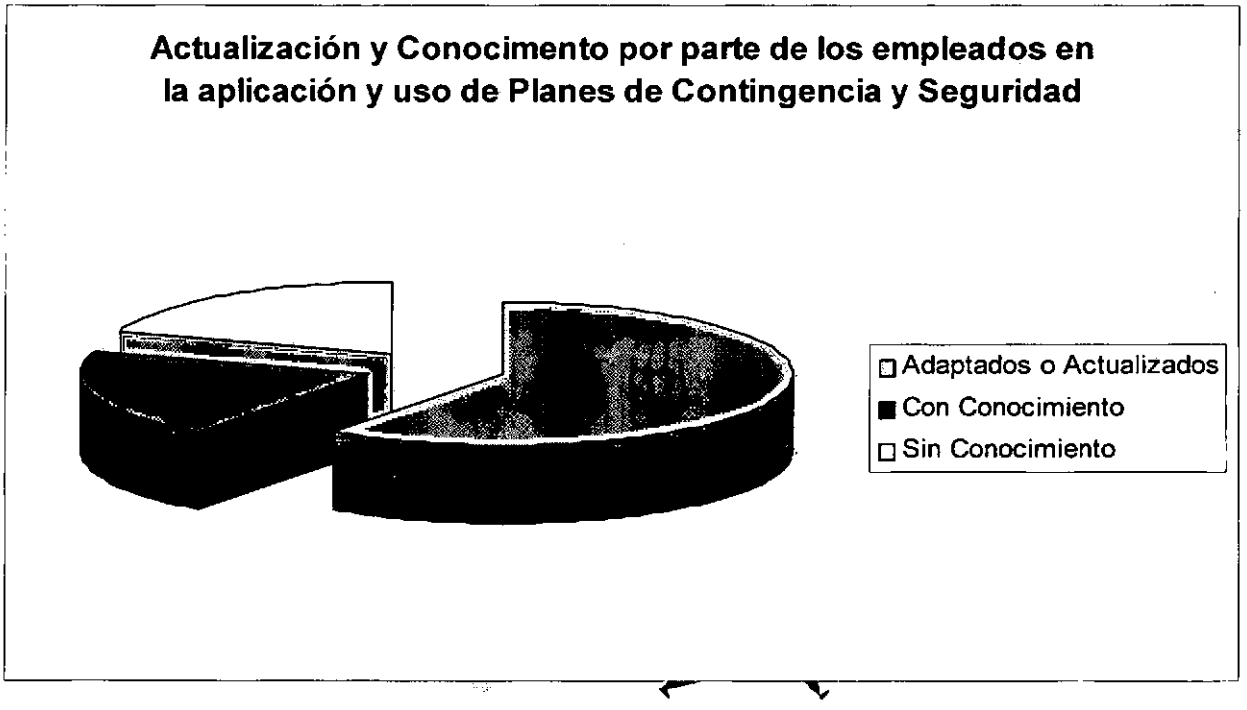


Figura N°3

Vemos claramente en la **Figura N°3** que mas de la mitad de la organizaciones tienen actualizados los requerimientos necesarios para estar prevenidos, pero que lamentablemente el uso no será el adecuado por la falta de conocimiento parcial o total de los empleados de estas organizaciones .

3.2. Requisitos Mínimos para la Elaboración de Planes de Contingencias

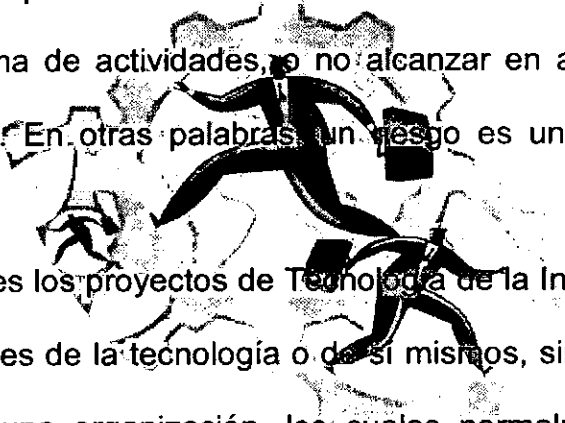
3.2.1 Plan de Reducción de Riesgos

Para asegurar que se consideran todas las posibles eventualidades, se debe realizar un análisis de riesgos.

La evaluación de los riesgos y presentación de repuestas debe prepararse en forma personalizada para cada organización, de esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

Análisis de Riesgo

Un riesgo es la posibilidad de sufrir una pérdida. Para un proyecto específico, el percance puede ser un producto terminado con menor calidad, costos más elevados, retrasos en el programa de actividades, o no alcanzar en absoluto el propósito y la intención del proyecto. En otras palabras, un riesgo es un problema en espera de ocurrir.

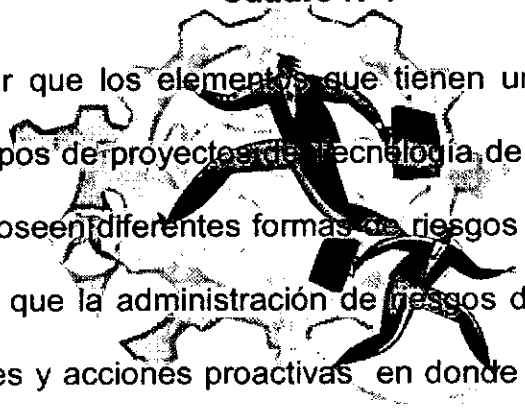


Para las Organizaciones los proyectos de Tecnología de la Información, en su mayoría fracasan, no por razones de la tecnología o de sí mismos, sino por las presiones a un nivel más amplio de una organización, los cuales normalmente se ignoran. Estas presiones adoptan muchas formas, como actividades de los competidores, estabilidad financiera y cultura de la organización, la manera de poder observar mejor estas situaciones de la Organización, se describen las fuentes del riesgo y sus posibles consecuencias en el **Cuadro N°1**.

Categorías de fuentes de riesgo.	**Consecuencias en el proyecto.**
Propósito y metas.	Costos excesivos.
Necesidad de tomar decisiones.	Retrasos en las actividades.
Administración de la organización.	Funcionalidad inadecuada.
Cliente usuario final.	Proyectos cancelados.

Presupuestos / costos.	Cambios repentinos de personal.
Programa de actividades.	Insatisfacción del cliente.
Características del proyecto.	Deterioro de la imagen de la compañía.
Proceso de desarrollo.	Personal desmoralizado.
Ambiente de desarrollo.	Rendimiento deficiente del producto.
Personal.	Procesos legales.
Ambiente operativo.	Tecnología nueva.

Cuadro N°1



Es interesante señalar que los elementos que tienen un riesgo significativo no son iguales en todos los tipos de proyectos de Tecnología de la Información. Las diversas clases de proyectos poseen diferentes formas de riesgos y deben abordarse en forma individual. Es por eso que la administración de riesgos desarrolla una disciplina y un ambiente de decisiones y acciones proactivas en donde se consideran dos enfoques inherentemente distintos para la administración, uno es reactivo y el otro es proactivo.

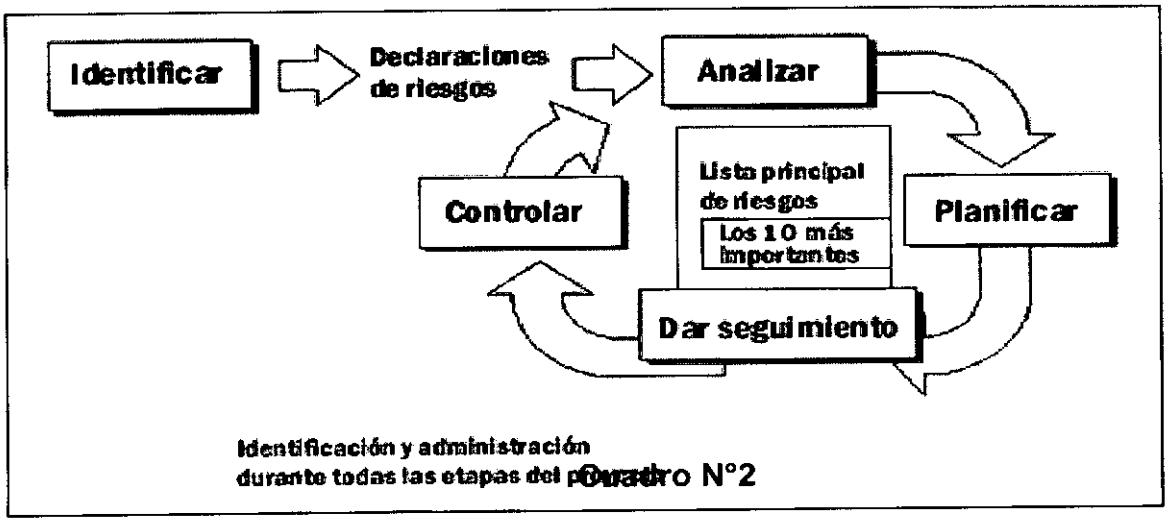
La administración reactiva de riesgos, significa que el equipo del proyecto reacciona a las consecuencias de los riesgos (los problemas reales) conforme ocurren. La administración proactiva de riesgos, significa que el equipo del proyecto cuenta con un proceso visible para administrarlos. Este proceso se puede medir y repetir.

La prevención del riesgo es el punto de transición entre estos enfoques. La prevención ocurre en las etapas de planeación de un proyecto, cuando el equipo puede aplicar acciones para impedir que ocurran los riesgos. Es importante señalar que, esencialmente, la prevención es todavía una estrategia reactiva para administrar los

riesgos; no es un remedio para la causa del riesgo, sólo una forma de evitar sus síntomas.

Para alcanzar los niveles más altos de la administración proactiva de riesgos, el equipo debe estar dispuesto a tomar riesgos. Esto significa no temer el riesgo, sino considerarlo como un medio para crear oportunidades adecuadas. Para conseguirlo, el equipo debe ser capaz de evaluar imparcialmente los riesgos (y las oportunidades) y, a continuación, aplicar acciones que aborden las causas de estos, no sólo sus síntomas. Pensemos que *"El factor determinante para tener éxito no es la calidad de la valoración del riesgo, sino la capacidad del personal para administrar el riesgo y la oportunidad. "*

Cuando el equipo del proyecto emplea la administración proactiva de riesgos, los valora en forma continua y los utiliza para tomar decisiones en todas las etapas del proyecto. Incluye los riesgos y los enfrenta hasta que se resuelven o hasta que se convierten en problemas y se manejan como tales. Los pasos para este tipo de administración serían los que se observan en el **Cuadro N°2** y en consiguiente su desarrollo.



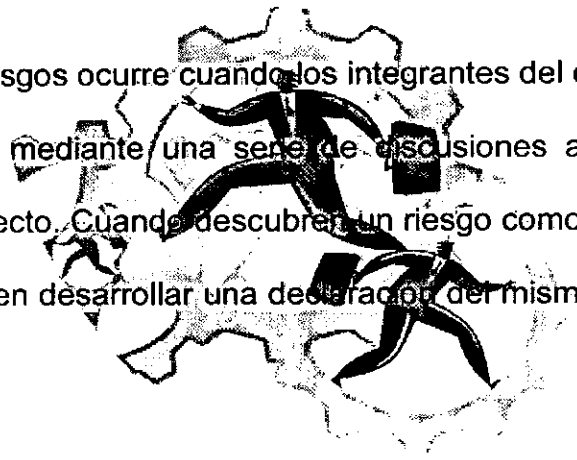
Cuadro N°2

A- Identificación de riesgos

Es el primer paso en el proceso de la administración proactiva de riesgos. (deben identificarse antes de que puedan administrarse). La identificación de los mismos

proporciona las oportunidades, indicios e información que permiten ubicar los riesgos principales antes de que afecten adversamente al proyecto. El proceso que ocurre entre los integrantes del equipo que identificara los riesgos es muy importante. Es un medio vigoroso de manifestar las suposiciones y los puntos de vista contrastantes.

No es probable que en un equipo haya coincidencia en la valoración de todos los factores de riesgo. Dependiendo de su experiencia, cada uno de los diferentes integrantes del equipo tendrá una opinión propia. Si después de una discusión no se alcanza un acuerdo, el mejor enfoque es una votación, en donde prevalece la opinión de la mayoría.



La identificación de riesgos ocurre cuando los integrantes del equipo emplean tablas de factores de riesgo y, mediante una serie de discusiones abiertas, los identifican y clasifican para el proyecto. Cuando descubren un riesgo como resultado de ponderar la tabla de factores, deben desarrollar una declaración del mismo e introducirla en la lista principal de riesgos.

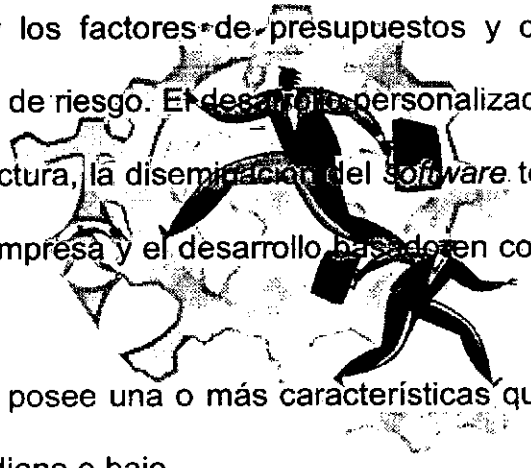
Por Ejemplo:

Factor de riesgo.	**Señal de riesgo bajo.**	**Señal de riego mediano.**	**Señal de riesgo alto.**
Conveniencia de la organización o proyecto	Apoya directamente las metas y propósitos de los clientes o usuarios.	Afecta indirectamente una o más metas.	No apoya ni se relaciona con el propósito o las metas del cliente o usuario.
Percepción del cliente o usuario.	Espera que el equipo genere este producto.	Piensa que el equipo no trabaja en el producto esperado.	Cree que el producto deseado no coincide con los productos anteriores del

			equipo.
Desarrollo de las actividades.	Provoca muy poco o ningún cambio en el desarrollo de las actividades.	Cambia ciertos aspectos o afecta mínimamente el desarrollo de las actividades.	Modifica sustancialmente el desarrollo de las actividades o el método de la organización.

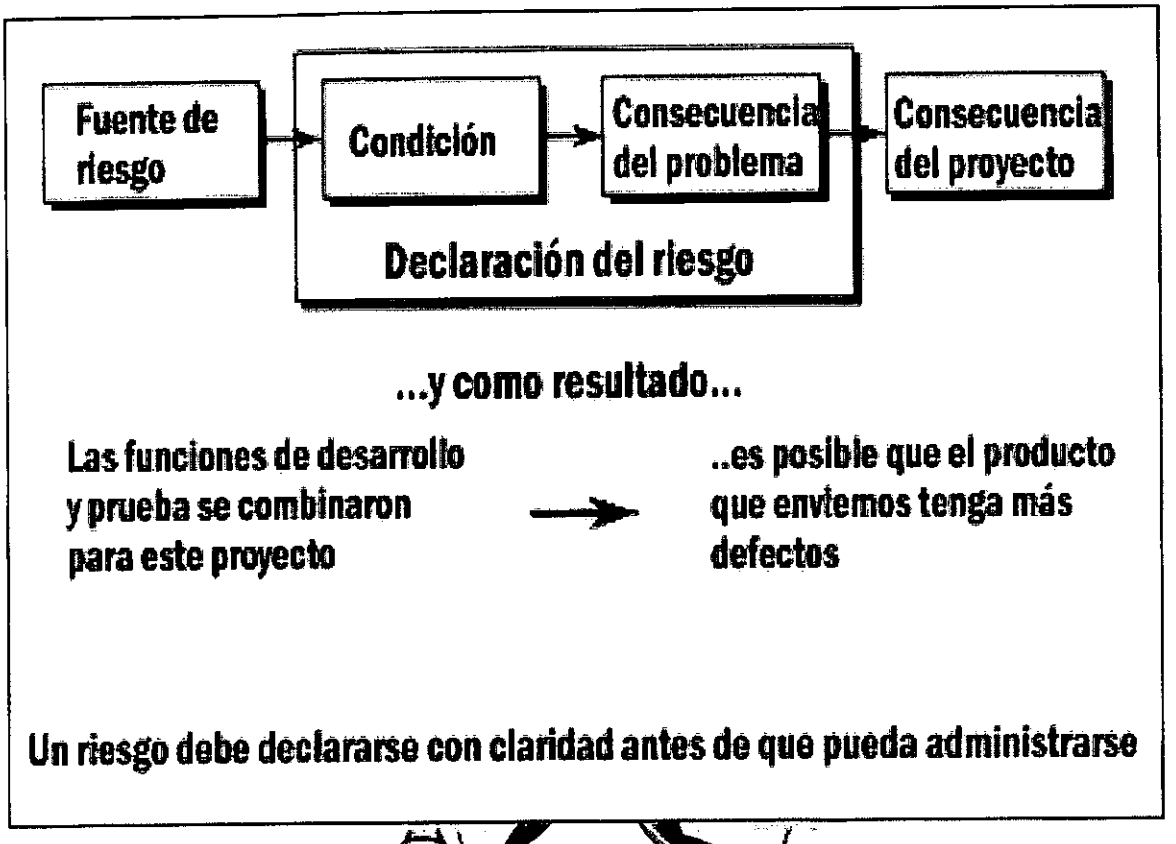
Cuadro N°3: Factores de riesgo del propósito y las metas.

Los factores de riesgo se agrupan por área de atención y categoría. Los factores del propósito y las metas, la necesidad de tomar decisiones, los factores de administración de la organización, y los factores de presupuestos y costos son ejemplos de las categorías de factores de riesgo. El desarrollo personalizado de *software*, el despliegue rápido de la infraestructura, la diseminación del *software* terminado, la planificación de la arquitectura de la empresa y el desarrollo basado en componentes son ejemplos de áreas de atención.



Cada factor de riesgo posee una o más características que describe si el riesgo debe considerarse alto, mediano o bajo.

Antes de que pueda administrarse, debe expresarse con claridad. Cuando se declara un riesgo, no se debe considerar sólo un síntoma, sino también un resultado. Por esa razón, la declaración del riesgo debe incluir lo que provoca que surja la situación (esto es, la condición) y el resultado esperado (la consecuencia).



Cuadro N° 4

B- La declaración y análisis del riesgo.

La conversión de los datos de un riesgo a información es la forma en que se declaran los riesgos para la toma de decisiones respectiva. Un análisis minucioso corrobora que el equipo trabaja en los riesgos convenientes.

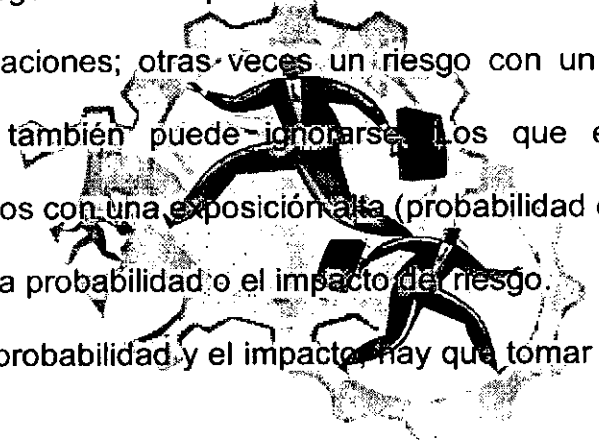
Una vez declarado, tenemos que se compone de dos factores: su **probabilidad** y su **impacto**. La **probabilidad** de un riesgo es la posibilidad de que un evento suceda en realidad. Para clasificarlos es recomendable la asignación de un valor numérico a la probabilidad. La misma debe ser mayor que cero o el riesgo no representa una amenaza para el proyecto. Asimismo, la probabilidad debe ser menor que 100% o el riesgo es una certeza, en otras palabras, es un problema identificado.

El **impacto** de un riesgo mide la severidad de los efectos adversos, o la magnitud de una pérdida, si llega a suceder. En el caso de que el impacto sea financiero, el valor

monetario es la forma preferible para cuantificar la magnitud de una pérdida. Este, podrían ser costos a largo plazo en la operación y el apoyo, una pérdida en la participación en el mercado, costos a corto plazo por el trabajo adicional, o pérdida en el costo de oportunidad.

Otros riesgos pueden tener un nivel de impacto en donde es más conveniente una escala subjetiva del 1 al 5. Los valores altos indican una pérdida seria para el proyecto. Los valores medianos señalan una pérdida en partes o una disminución de la eficiencia.

En ocasiones un riesgo con una probabilidad alta tiene un impacto bajo y puede ignorarse sin complicaciones; otras veces un riesgo con un impacto alto tiene una probabilidad baja y también puede ignorarse. Los que en verdad se requiere administrar son aquellos con una exposición alta (probabilidad e impacto altos). Esto se consigue reduciendo la probabilidad o el impacto del riesgo.



Cuando se estime la probabilidad y el impacto, hay que tomar en cuenta lo que sabe y lo que desconoce.

La siguiente es una lista de la información que el equipo debe considerar cuando se desarrolle un formulario de declaración de riesgos:

- *Identificador del riesgo.* El nombre que se emplea para identificar inequívocamente una declaración de riesgo, con el propósito de elaborar informes y darle seguimiento.
- *Fuente del riesgo.* El área de atención (esto es, el desarrollo personalizado de software, la diseminación del *software* terminado, el despliegue de la infraestructura, la administración del programa de la empresa o la planificación de la arquitectura de la empresa), la categoría del factor de riesgo (esto es, el propósito y las metas, la necesidad de tomar decisiones, la administración de la

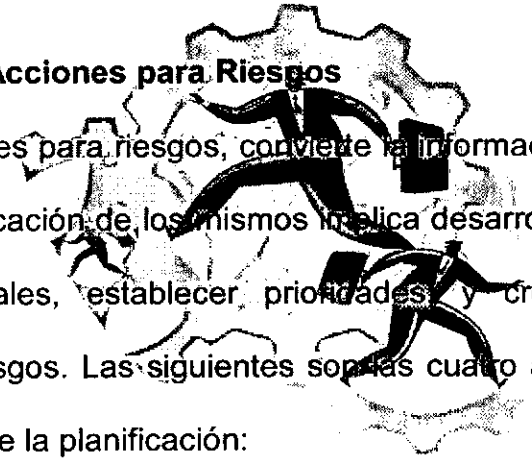
organización, el programa de actividades, o el presupuesto/costo), y el factor de riesgo (esto es, la conveniencia del proyecto, la influencias políticas, la estabilidad de la organización, el tamaño del proyecto) que se emplearon para identificar el riesgo.

- *Condición del riesgo.* Una declaración en lenguaje normal que describa una condición existente que pudiera conducir a una pérdida.
- *Consecuencia del riesgo.* Una declaración en lenguaje normal que describa la pérdida que ocurriría si se materializara el riesgo.
- *Probabilidad del riesgo.* Una expresión del porcentaje mayor que cero y menor que el 100 por ciento que representa la probabilidad de que la condición ocurra en realidad, provocando una pérdida.
- *Clasificación del impacto del riesgo.* Si el impacto del riesgo es, por ejemplo, financiero, estratégico, técnico o legal.
- *Impacto del riesgo.* La magnitud del impacto en caso de que el riesgo ocurra en realidad. Este número debe ser el valor monetario de la pérdida o simplemente un número entre 1 y 10 que represente una magnitud relativa. Para valorarlo, a menudo se emplea el resultado de multiplicar el impacto por la probabilidad del riesgo.
- *Exposición al riesgo.* La amenaza completa que significa el riesgo para el proyecto, compensando la probabilidad de una pérdida real con la magnitud de la pérdida posible.
- *Contexto del riesgo.* Un párrafo con antecedentes adicionales que sirvan para aclarar la situación del riesgo.
- *Riesgos relacionados.* Una lista de identificaciones que emplea el equipo para dar seguimiento a los riesgos que dependen entre sí.

El análisis de riesgos pondera la amenaza de cada riesgo como una ayuda para decidir en cuáles riesgos es conveniente aplicar una acción. Lo fundamental es identificar una cantidad limitada de riesgos importantes que deben administrarse (por lo general 10 o menos). Para clasificar la exposición del riesgo, todos los valores de impacto deben estar en las mismas unidades de medición, ya sean valores monetarios o niveles de impacto.

Después de clasificarse, se debe generar una estrategia de administración del mismo y la forma de incorporar los planes de acción para un riesgo en el plan general de la organización.

C- Planificación de Acciones para Riesgos



Los planes de acciones para riesgos, convierte la información del riesgo en decisiones y acciones. La planificación de los mismos implica desarrollar acciones para enfrentar los riesgos individuales, establecer prioridades, y crear un plan integrado de administración de riesgos. Las siguientes son las cuatro áreas fundamentales que se deben abordar durante la planificación:

- *Investigación.* ¿Conocemos lo suficiente acerca de este riesgo? ¿Necesitamos estudiar más el riesgo para adquirir más información y determinar mejor sus características antes de que podamos decidir qué acción efectuar?
- *Aceptación.* ¿Podemos soportar las consecuencias si el riesgo ocurriera en realidad? ¿Podemos aceptar el riesgo y no aplicar más acciones?
- *Administración.* ¿Se puede hacer algo para atenuar el impacto del riesgo en caso de que ocurra?
- *Prevención.* ¿Podemos evitar el riesgo cambiando el campo?

Es importante considerar que las tres metas de la administración de riesgos son; Reducir la probabilidad de ocurrencia, la magnitud de una pérdida y modificar las

consecuencias del riesgo que mediante algunas de las siguientes estrategias podremos decir que en:

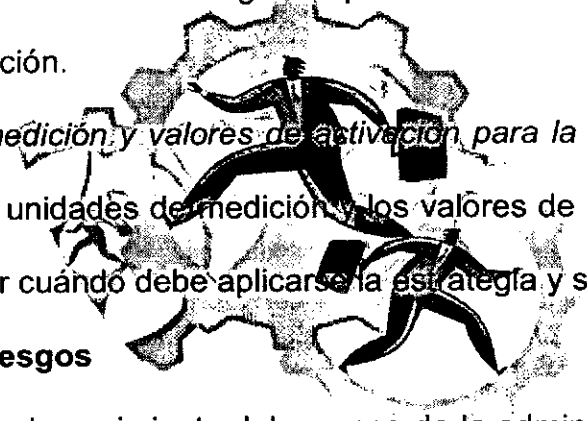
- En los riesgos que se puedan controlar, se deben aplicar los recursos necesarios para reducirlos.
- En los riesgos que no se pueden controlar, determinar cambios de estrategia.
- Es posible que se transfiera el riesgo mediante:
  - El cambio a un hardware distinto.
  - El traslado de una característica del software a otra parte del sistema que posea mejor capacidad para manejarla.
  - La subcontratación de la tarea con un profesional más experimentado.

La idea detrás de una estrategia es contar con un plan de reserva que pueda activarse en caso de que fracasen todos los esfuerzos para administrar el riesgo.

La siguiente es una lista de la información que se podría considerar al desarrollar un formulario de acciones automatizadas para el riesgo:

- *Identificador del riesgo.* Idem Formulario de Declaración de Riesgos
- *Declaración del riesgo.* La declaración en lenguaje normal (que se explicó antes) que describa la condición existente que podría conducir a una pérdida y la descripción de la pérdida que ocurriría si el riesgo se volviera una certeza.
- *Estrategia de administración del riesgo.* Un párrafo o dos que describa la estrategia para administrar el riesgo, en donde se incluyan las suposiciones consideradas.
- *Unidades de medición para la estrategia de administración del riesgo.* Las unidades de medición que se usaran para determinar si funcionan las acciones planeadas para la administración del riesgo.

- *Conceptos de las acciones.* Una lista de las acciones que se aplicarán para administrar el riesgo.
- *Fechas de entrega.* La fecha en que se terminará cada concepto de una acción planificada.
- *Asignaciones de personal.* Las personas asignadas para ejecutar los conceptos de las acciones.
- *Estrategia de prevención del riesgo.* Un párrafo o dos que describa la estrategia en caso de que no funcionen las acciones planificadas para administrar el riesgo. Se ejecutaría la estrategia de prevención del riesgo si se alcanzara su punto de activación.
- *Unidades de medición y valores de activación para la estrategia de prevención del riesgo.* Las unidades de medición y los valores de activación que se usarán para determinar cuándo debe aplicarse la estrategia y si ésta funciona.



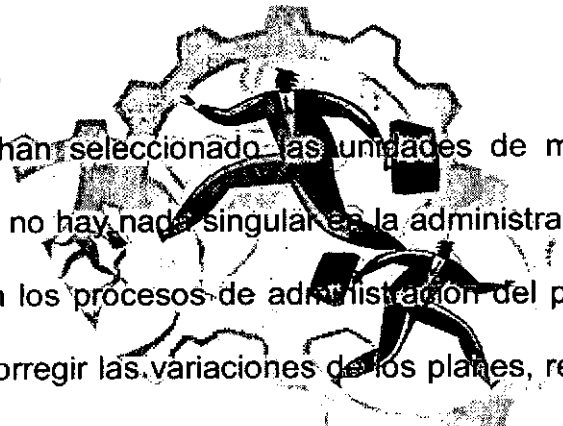
D- Seguimiento de riesgos

Es importante realizar el seguimiento del proceso de la administración de riesgos, para vigilar el estado y las acciones que se han aplicado para atenuarlos, incluyendo una revisión del mismo durante las revisiones y los análisis regulares del Proyecto. Esto debe incorporar una valoración del avance en la solución de los 10 riesgos más importantes.

Las revisiones se programan con regularidad (en forma mensual o en los puntos de decisión significativos), es útil mostrar la clasificación de riesgos anteriores, por ejemplo, la cantidad de veces que un riesgo ha estado en la lista de los 10 más importantes.

Para ello en la elaboración de informes del estado de riesgos se identifican cuatro situaciones posibles:

- Un riesgo se soluciona, con lo que termina el plan de acciones que le corresponde.
- Las acciones para un riesgo siguen el plan de administración de riesgos, en cuyo caso se mantienen dentro de lo planificado.
- Algunas acciones para un riesgo no siguen el plan de administración de riesgos, en cuyo caso deben determinarse e implementarse medidas correctivas.
- La situación ha cambiado significativamente en relación con uno o más riesgos y por lo general requerirá una revaloración de los riesgos o volver a planificar una actividad.



E- Control de riesgos

Después de que se han seleccionado las unidades de medición de riesgos y los eventos de activación, no hay nada singular en la administración de riesgos. Más bien, se debe combinar con los procesos de administración del proyecto para controlar los planes de acciones, corregir las variaciones de los planes, responder a los eventos de activación, y mejorar el proceso de administración de riesgos.

3.2.2. Plan de Recuperación de Contingencias

Es importante definir los procedimientos y planes de acción como se describió anteriormente para el caso de una posible falla, siniestro o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de una PC.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Organización.

Los procedimientos de planes de recuperación de contingencias deben de emanar de la máxima autoridad Organizacional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Contingencias se pueden clasificar en tres etapas.

3.2.2.1. Actividades Previas a la Contingencia

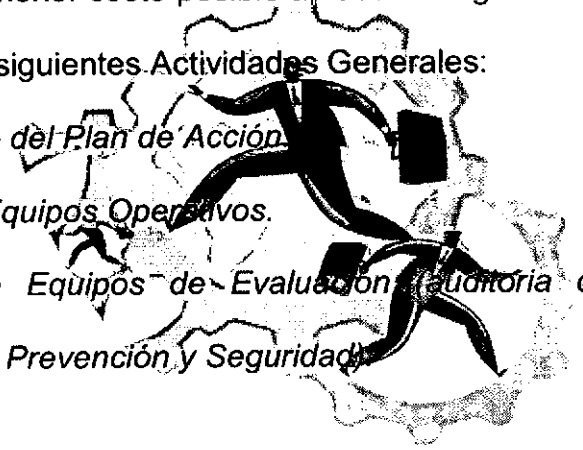
Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de Recuperación con el menor costo posible a nuestra Organización.

Podemos detallar las siguientes Actividades Generales:

A) Establecimiento del Plan de Acción.

B) Formación de Equipos Operativos.

C) Formación de Equipos de Evaluación (auditoria de cumplimiento de los procedimientos de Prevención y Seguridad).



A) Establecimiento de Plan de Acción

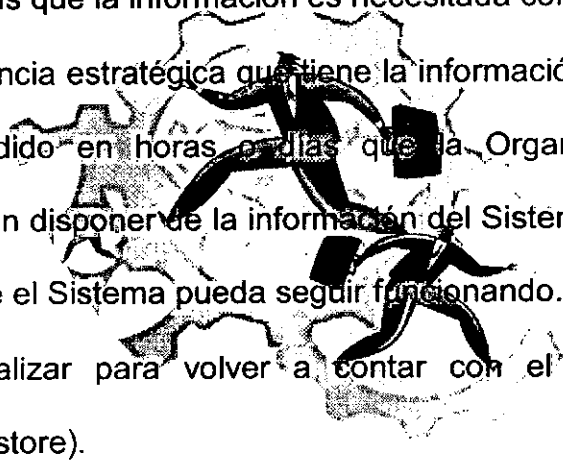
En esta fase de Planeamiento se debe de establecer los procedimientos relativos a:

Sistemas e Información: La Organización deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el área de sistemas como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para el buen funcionamiento Organizacional.

La relación de Sistemas de Información deberá detallar los siguientes datos :

- Nombre del Sistema.
- Lenguaje o Paquete con el que fue creado el Sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).

- La Dirección (Gerencia, Departamento, 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 Organización (medido en horas o días que la Organización puede funcionar adecuadamente, sin disponer de la información del Sistema). Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando.
- Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).



Con toda esta información se deberá de realizar una lista (un ranking) de los Sistemas de Información necesarios para que la Organización pueda recuperar su operatividad perdida en la contingencia.

Equipos Informáticos Inventario actualizado de los equipos de manejo de información (computadoras, cintas magnética, impresoras, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso organizacional.

- Pólizas de Seguros Comerciales. Como parte de la protección de los Activos de la organización, pero haciendo la salvedad en el contrato, que en casos de incidentes,

la restitución de las PC's destruidas se podrán hacer por otras de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.

- Señalización o etiquetado de las PC's de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.
- Tener siempre actualizada una relación de PC's requeridas como mínimo para cada Sistema permanente de la Organización (que por sus funciones constituyen el eje central de los Servicios Informáticos de la Organización), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Organización. Para lo cual se debe contar con :

1) Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

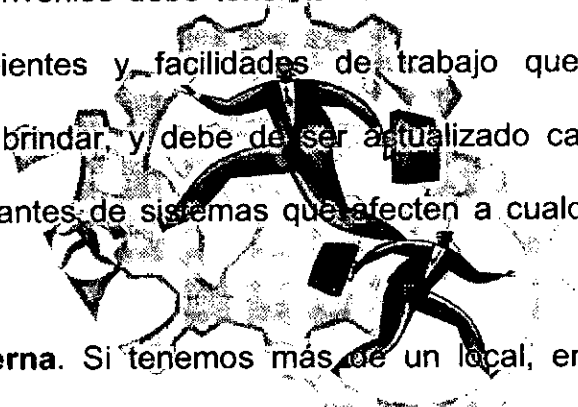
2) Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan los distintos Aplicativos de la Organización).

3) Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.

4) Backups de los Datos (Bases de Datos, Índices, tablas de validación, paswords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Organización).

5) Backups del Hardware. Se puede implementar bajo dos modalidades :

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



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

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

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

- Periodicidad de cada Tipo de Backup.
- Respaldo de Información de movimiento entre los períodos que no se sacan Backups (backups increméntales).
- Uso obligatorio de un formulario estándar para el registro y control de los Backups
- Correspondencia entre la relación de Sistemas e Informaciones necesarias para la buena marcha de la empresa (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 medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
- Almacenamiento de los Backups en locales diferentes donde reside la información primaria (evitando la pérdida si el incidente alcanzo todo el edificio o local estudiado).
- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

B) Formación de Equipos Operativos

En cada unidad operativa de la organización, que almacene información y sirva para la operatividad organizacional, se deberá designar un Referente informático para la seguridad de la Información de su unidad. Pudiendo ser el encargado de dicha Área Operativa.

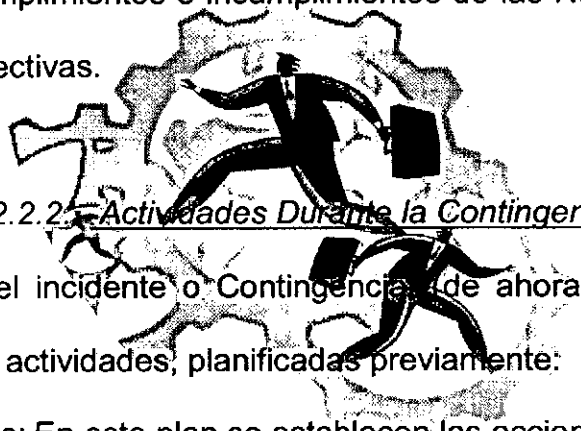
Sus labores serán:

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

C) Formación de Equipos de Evaluación (auditoria de cumplimiento de los procedimientos sobre Seguridad)

Esta función debe ser realizada de preferencia por personal externo, de no ser posible, la realizará el personal del área de Informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos :

- Revisar que las Normas y procedimientos con respecto a Backups y seguridad de equipos se cumpla.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Revisar la correlación entre la relación de Sistemas e Informaciones necesarios para la buena marcha de la Organización (detallados en «a»), y los backups realizados.
- Informar de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.



3.2.2.2 Actividades Durante la Contingencia

Una vez presentado el incidente o Contingencia (de ahora en mas I/C) se deberá ejecutar las siguientes actividades, planificadas previamente:

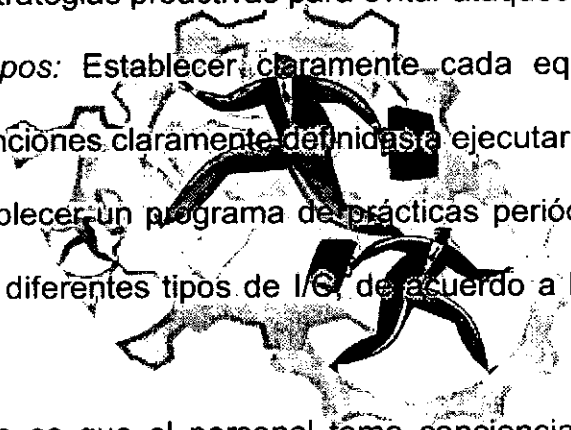
- *Plan de Emergencias:* En este plan se establecen las acciones que se deben realizar cuando se presente un I/C, así como la difusión de las mismas. Es conveniente prever los posibles escenarios de ocurrencia, durante el día, la Noche o madrugada.

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

- Deshabilitación del ingreso de los usuarios al sistema.
- Difundir a los usuarios los nuevos procedimientos para la ejecución de los sistemas, al momento del incidente y en adelante, utilizando mensajes de red y teléfonos a jefes de Área.

- Evaluación de las posibles causas, determinado por que tuvo lugar.
- Puesta en marcha de los procesos y procedimientos de restauración de la información. Plan de Acción.
- Documentación de todos los aspectos que se conozcan del mismo, entre los que se incluyen el daño que ha causado (en hardware y software, pérdida de datos o pérdida de productividad), los puntos vulnerables y las debilidades que se exploraron durante el ataque, la cantidad de tiempo de producción perdidos y los procedimientos tomados para reparar el daño. La documentación ayudará a modificar las estrategias proactivas para evitar ataques y futuros daños.

- *Formación de Equipos:* Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante un I/C.



- *Entrenamiento:* Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de I/C, de acuerdo a los roles que se le hayan asignado.

Un aspecto importante es que el personal tome conciencia de que los I/C, pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos, es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Organizacional.

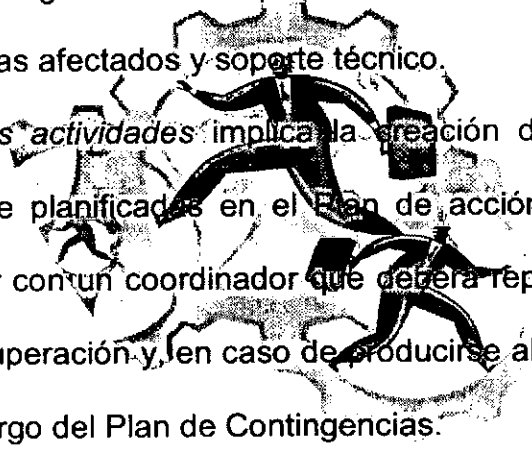
3.2.2.3. Actividad Después de la Contingencia

Oocurrido el I/C es necesario realizar la *Evaluación de Daños* inmediatamente después que el mismo ha concluido, en donde se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, en cuanto tiempo, etc.

Adicionalmente se deberá lanzar un preaviso a la Organización con la cual tenemos el convenio de respaldo, si lo hubiere, para ir avanzando en las labores de preparación de entrega de los equipos por dicha Organización.

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

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



La *ejecución de estas actividades* implica la creación de equipos de trabajo para realizarlas previamente planificadas en el Plan de acción (A1). Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato al Área a cargo del Plan de Contingencias.

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

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por los I/C, debemos de *evaluar objetivamente*, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias

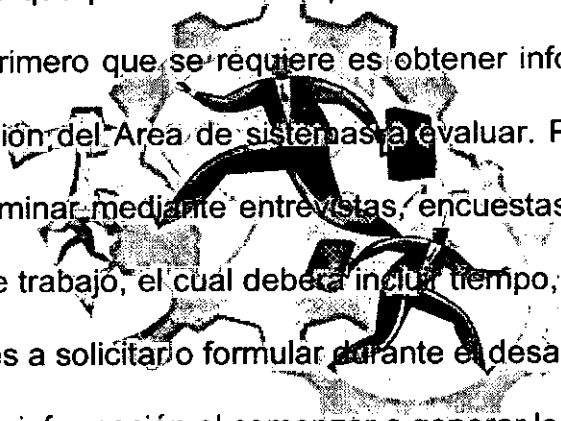
modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

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

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

4. RECOMENDACIONES

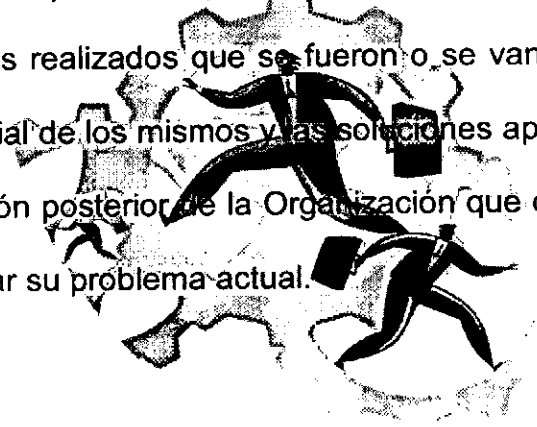
Se ha podido observar que para hacer una planeación eficaz de contingencias sobre una organización, lo primero que se requiere es obtener información general sobre la misma y sobre la función del Área de sistemas a evaluar. Para ello es preciso hacer una investigación preliminar mediante entrevistas, encuestas, etc. y con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.



Una vez obtenida dicha información el comenzar a generar los planes de Contingencias y seguridad teniendo en cuenta el estudio de los riesgos podemos recomendar finalmente que:

- Para el desarrolle un un plan de Contingencias es importante considerar que leyes o reglamentaciones a nivel Provincial y Nacional nos respaldan o nos fijan pautas.
- Proponer políticas de implementación y uso de estos planes para la Organización.
- Concientizar a los directivos de las distintas Organizaciones tanto públicas como privadas, que implementar un Plan de Contingencias es una inversión y no una perdida de tiempo.

- Difundir las pautas y procedimientos implementados para llevarlos a cabo, con el conocimiento general de todos los integrantes de la Organización.
- Considerar en primera medida que la información que maneja una Organización es la base para su funcionamiento y que si no es prevenida su seguridad y reconstitución, no se puede pensar en el futuro de la misma.
- Realizar las tareas que hallan sido programadas para el mantenimiento de los equipos, que en cierta forma disminuye que surjan imprevistos.
- Es muy importante que se realice la documentación de todos los incidentes realizados que se fueron o se van presentando para formular un historial de los mismos y las soluciones aplicadas o posibles, para una prevención posterior de la Organización que cuente con antecedentes en que basar su problema actual.



5. BIBLIOGRAFÍA

- Informe Parcial Actividad 9.0 Proyecto Redes **"RELEVAMIENTO INTEGRAL DEL FUNCIONAMIENTO DEL ESTADO PROVINCIAL EN EL MANEJO DE LA INFORMACIÓN"** San Luis.
- **INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA** (INEI) del Perú.
- **MICROSOFT TECHNET -** Sitio en Internet - http://www.microsoft.com/latam/technet/admon/estrategia
- **LA FACU** – Sitio de Internet – http://www.lafacu.com/apuntes/informatica/manu_audit_sist
- **SOFTWARE ENGINEERING INSTITUTE**

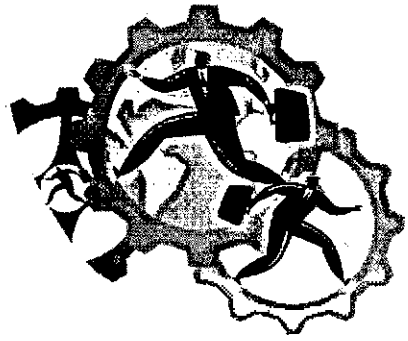
  Microsoft Solutions Framework, en http://www.microsoft.com/msf/

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

ELABORACIÓN DE PLANES DE CONTINGENCIA



ACTIVIDAD 2

"ESTUDIO Y ANÁLISIS DE LAS NORMAS Y REGLAMENTACIONES ADOPTADAS POR EL GOBIERNO PROVINCIAL"

"ESTUDIO Y ANÁLISIS DE LAS NORMAS Y REGLAMENTACIONES ADOPTADAS POR EL GOBIERNO PROVINCIAL"

Índice

1. Enunciado
2. Objetivo
3. Cuerpo
   3.1. Estudio previo de la situación general
   3.2.Investigación
   3.3. Análisis
4. Conclusiones
5. Bibliografía

1. ENUNCIADO

La generalización del uso de las tecnologías de la información y de las comunicaciones es potencialmente beneficiosa para los ciudadanos, las empresas y la propia Administración Pública, pero también da lugar a riesgos que deben minimizarse con medidas de seguridad y planes de contingencia que generen confianza en su utilización y, por lo tanto, en los servicios brindados.

No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para, así implantar las medidas proporcionadas a estos riesgos, al estado de la tecnología y a los costos, tanto de la ausencia de seguridad como de las salvaguardas (Ver actividad 1 del contrato "Políticas de Mitigación de Riesgos").

A medida que la tecnología ha ido evolucionando y con ella, la envergadura de los sistemas de información de las organizaciones públicas y privadas, la seguridad del entorno informático (hardware, software, comunicaciones, etc.) se ha convertido en una de las grandes preocupaciones de los profesionales de esta actividad. Esta preocupación debe ser adecuadamente comprendida y compartida por los directivos, los cuales deben considerar a las inversiones en medidas de seguridad informática, como un gasto necesario, que contribuye a mantener la operatividad y rentabilidad de las Organizaciones tanto públicas como privadas.

Esto implica que los responsables del Servicio Informático, deban explicar con la suficiente claridad y con un lenguaje inteligible, las potenciales consecuencias de una política de seguridad insuficiente o incluso inexistente. La presente actividad, en intima relación con la anterior y posterior, pretende ayudar a comprender mejor la necesidad implícita de los sistemas de información soportados por una PC, de las medidas de seguridad adecuadas, tanto en su número como en su rigor y nivel de aplicación, ya que toda Organización debe estar preparada para el caso de ocurrencias imprevistas.

Para poder llegar a un modelo genérico es necesario enmarcarse en el marco legal vigente dentro del ámbito Provincial y Nacional que conlleve una incidencia a la provincia. Es por esto que se ha encarado este análisis.

2. OBJETIVO

Estudio y análisis de las normas y reglamentaciones adoptadas en la actualidad por el Gobierno Provincial para enmarcar los planes de contingencia en un todo de acuerdo con las mismas.

3. CUERPO

3.1. Estudio previo de la situación general

El mundo informático se enfrentó con un grave riesgo o, dicho de otra manera, con una contingencia de alto riesgo, con el advenimiento del Año 2000. Con él surgió el concepto y la urgencia de generar planes de contingencias a fin de no llegar a situaciones de emergencia.

Hay cientos de documentos generados con el ya conocido problema del Y2K que atestiguan la falta de previsión y conocimiento con respecto a contingencias imprevistas.

"Es de conocimiento público que grandes organizaciones, empresas, instituciones, así como dependencias y organismos gubernamentales se han dado ya a la tarea de convertir sus equipos informáticos y demás equipo computarizado para evitar cualquier problema antes mencionado o cualquier otro no esperado. Piense en el riesgo que corre su organización o empresa si no se toman medidas para cerciorarse si es blanco o no de este potencial problema." Informática Integral México - Publicado en www.geocities.com/Eureka/Office/4595/y2k.html

"...admitiendo que el problema afectará a todo aquello que "use chips con funciones de fechas", como ser computadoras, edificios, generadores o distribuidores de energía, acondicionadores de clima, ascensores, aviones, equipos médicos, implantaciones médicas, máquinas herramientas, equipos de transporte, etc.; por lógica afectará la actividad comercial, técnica, administrativa, financiera, legal, productiva, social, personal y otras; ¿entonces puede alguien decir, "Esto a mí no me involucra?".

Si bien estamos frente a un problema universal que afectará a personas y organizaciones sin distinción geográfica, la idiosincrasia, usos y costumbres de algunos países, presentan aquí características propias." Argentina. Publicado en : http://www.2000.com.do/argentina/welcome.htm

"Aún si el hardware y el sistema operativo estuvieran bien, los programas financieros personales, las aplicaciones contables, las hojas electrónicas o las bases de datos podrían malinterpretar las fechas o manipular archivos de datos con ingresos inconvenientemente digitalizados, lo que causaría serios problemas.

Ya que la ignorancia y el manejo de conceptos equivocados sobre el problema son los mayores enemigos del tomador de decisiones, ponemos a su disposición está y las siguientes áreas de conocimiento sobre el Y2K." Tecnología Latinoamericana S. - Honduras. Publicado en: http://www.webito.com/y2k/index.html

"Desde la más pequeña hasta la más grande, las instituciones financieras de Idaho (bancos, instituciones de ahorro y uniones de crédito) han estado trabajando duro durante varios años para asegurarse de que los sistemas de computadoras funcionen correctamente en el año 2000 (Y2K). Además, los reguladores estatales y federales están controlando muy de cerca el progreso de las instituciones que supervisan para asegurarse de que los problemas del Y2K están siendo tratados. A pesar de todos los esfuerzos de la industria y de los reguladores, nadie puede garantizar que todo va a funcionar perfectamente" USA – The Official Web Site of Idaho – Publicado en: http://www2.state.id.us/finance/y2k/y2kchkep.htm

En un panorama general de pánico al inicio y planificación organizada posterior se fueron organizando a nivel mundial los planes de contingencias para subsanar el efecto del Año 2000, con un grado de resolución y certeza altísimos, dado que no hubo, como se suponía, caídas de sistemas importantes dentro del espectro mundial.

Con este punto de partida las organizaciones comenzaron a plantar las bases para generar planes de contingencia y seguridad, como modelos a seguir en situaciones de emergencia previsibles (con cierto grado de imaginación), aun cuando hay riesgos que

no pueden preverse. Y también a nivel gubernamental comenzaron a surgir chispazos de pautas y propuestas para estandarizar y normalizar los mismos.

3.2. Investigación

Después de una extensa investigación no se han encontrado normas dirigidas explícitamente a la generación de planes de contingencia pero si se ha podido observar una previsión hacia la formación de equipos técnicos que se conviertan en originadores de las pautas y normas necesarias. Se incorporarán a continuación los extractos de las leyes correspondientes:

DECRETO NACIONAL 993/91 T.O. por RES. 299/95 (S.F.P.)

SISTEMA NACIONAL DE LA PROFESIÓN ADMINISTRATIVA.

Que la medida propuesta armoniza con los esquemas adoptados por los países avanzados en la materia, consagrando en su articulado la diversidad de Institutos propios de la carrera administrativa basada en modernas técnicas de gestión gerencial y profesionalización en todo su desarrollo

ANEXO A : CUERPO NORMATIVO

Art. 1.– El presente sistema Nacional consta de TRES (3) agrupamientos, denominados General, Científico-Técnico y Especializado.

Art. 13 .- Corresponde a funciones de planeamiento, organización y control en unidades organizativas y funciones de investigación o desarrollo tecnológico de máxima relevancia o complejidad, que impliquen la participación en la formulación de políticas

específicas, planes y cursos de acción en el campo científico o tecnológico y formación de recursos humanos altamente especializados.

DECRETO NACIONAL 2.295/93

CREACIÓN DEL INSTITUTO FEDERAL DE ASUNTOS MUNICIPALES.

Que la Reforma del sector estatal es un proceso que no se agota en la modernización del sector público nacional sino que debe ser acompañado por transformaciones profundas en las provincias y en los municipios.

Art. 2.- Serán objetivos del Instituto:

i) promover la implementación y el desarrollo de sistemas de control de la gestión municipal de servicios públicos, por la comunidad.

Art. 9. – El Instituto deberá contar con una Unidad de Investigación y Asistencia Técnica Recíproca, que tienda a desarrollar tecnologías específicas para Gobiernos Municipales.

LEY 25.154

APROBACION DE UN CONVENIO CON RUSIA SOBRE COOPERACION CIENTIFICA Y TECNICA

ARTICULO 1:

El objetivo del presente Convenio es contribuir a ampliar y profundizar los vínculos entre las comunidades científicas y técnicas de ambos países, mediante la creación de condiciones favorables para el desarrollo de la cooperación, sobre bases mutuamente beneficiosas y equilibradas.

ARTICULO 3:

La cooperación podrá incluir lo siguiente:

a.- intercambio de delegaciones de especialistas y de científicos;

b.- celebración de seminarios, conferencias y encuentros científicos conjuntos;

c.- formación y perfeccionamiento de científicos y especialistas;

d.- intercambio de información científica y tecnológica;

e.- realización conjunta de proyectos e investigaciones;

f.- cualquier otra forma de cooperación que ambas Partes puedan convenir.

En condiciones similares de cooperación científica y tecnológica, han sido firmados durante los últimos 10 años contratos con:

Finlandia (Ley 22.586), Brasil (Ley 22.457), Polonia (Ley 22.029), Gabon (Ley 21.942), Bolivia (Ley 21.820), Croacia (Ley 24724), Portugal (Ley 22.800), Honduras (Ley 22.791), Guatemala (Ley 2.692).

LEY 23.443

APROBACION DEL ACTA CONSTITUTIVA DE LA RED DE INFORMACION TECNOLOGICA LATINOAMERICANA (RITLA).

ARTICULO 1

La Red de Información Tecnológica Latinoamericana en adelante denominada RITLA, es un instrumento descentralizado de cooperación regional abierto a la participación de los Estados Miembros del Sistema Económico Latinoamericano, SELA y destinado a contribuir al desarrollo tecnológico regional a través del intercambio de información.

ARTICULO 2

Los objetivos fundamentales de la RITLA son:

a) Apoyar el desarrollo de las infraestructuras y sistemas de información tecnológica de los Estados Miembros y promover su aprovechamiento integral por los sectores gubernamental y privado:

b) Promover la coordinación y cooperación permanentes para que el intercambio de información tecnológica se efectúe de conformidad con las necesidades de los países participantes;

c) Reforzar las capacidades nacionales y regionales para la generación de tecnologías propias;

d) apoyar y mejorar la capacidad de los Estados Miembros para la búsqueda, selección, negociación, evaluación, adaptación y utilización de tecnologías importadas;

e) Impulsar la formación y capacitación de los recursos humanos requeridos para el desarrollo tecnológico de los Estados Miembros;

f) Promover el intercambio de la información técnico-económica que permita reforzar el vinculo entre la oferta y demanda de tecnología regional;

g) Promover la cooperación tecnológica entre los Estados Miembros a través de la difusión de las oportunidades existentes y de otras acciones que respondan a los problemas y desafíos derivados de la cooperación regional;

h) Establecer vínculos operativos con otros sistemas o redes de información tecnológica internacionales, regionales y subregionales.

Frente al problema que ya hemos mencionado del Año 2000 (Conocido como efecto Y2K) se generaron algunos decretos de los cuales extractamos aquellos ítems que comienzan el camino hacia la formación de planes de contingencia.

DECRETO NACIONAL 1402/99

ORGANISMOS ENCARGADOS DE LAS MEDIDAS DE EMERGENCIA FRENTE A LA POSIBLE CRISIS DEL AÑO 2000.

Considerando:

Que por el aludido Decreto se declaró en estado de alerta a todos los sistemas informáticos, y aún aquellos no informáticos pero cuyas prestaciones dependan de dispositivos electrónicos que puedan verse afectados en su funcionamiento a causa de la llamada crisis del año 2.000, disponiendo una serie de medidas estableciendo un sistema de responsabilidades específico para sancionar las omisiones o dilaciones en el cumplimiento de las normas e instrucciones dictadas y a dictarse con relación al problema del año 2.000 por parte de las entidades prestadoras de servicios. *Que no obstante las disposiciones contenidas en la citada norma, resulta necesario prever acciones referentes a la protección de la ciudadanía ante la posible falla de los planes de contingencias en servicios críticos causadas por el efecto aludido precedentemente.*

Que a tal fin el ESTADO NACIONAL debe tomar los recaudos necesarios que le permitan responder debidamente a las posibles consecuencias de fallas en servicios críticos para la población.

Que en tal sentido, existen organismos en el ámbito de la Administración Pública Nacional con disponibilidad de recursos humanos y materiales adecuados para encarar tales situaciones, constituyendo la JEFATURA DE GABINETE DE

MINISTROS el ámbito de coordinación de acciones que involucran las distintas áreas de Gobierno.

Que entre los recaudos a adoptar se encuentran los relativos a previsiones vinculadas al otorgamiento de licencias anuales ordinarias en el período crítico, así como la revisión del estado de mantenimiento de equipos tales como generadores eléctricos portables u otros y la provisión de insumos vitales como agua potable.

DECRETO NACIONAL 1004/99

DECRETO DE NECESIDAD Y URGENCIA SOBRE SISTEMAS INFORMATICOS

Que existe preocupación por parte del Poder Ejecutivo Nacional a causa de la llamada crisis del año 2000, respecto del funcionamiento de los sistemas informáticos, y aún de aquellos no informáticos pero cuyas prestaciones dependan de dispositivos electrónicos, correspondientes a las empresas del sector público o privado directamente vinculadas a la prestación de servicios públicos, ya sea en el carácter de concesionarias, licenciatarias, permisionarias o en virtud de cualquier otro título que las vincule con el Estado Nacional.

Que conforme a la situación descripta y ante el riesgo de que se vea afectado el normal desenvolvimiento de las actividades y servicios aludidos, con los consecuentes perjuicios para la sociedad en general, se torna necesario la adopción de medidas que definan un sistema de responsabilidades específico para sancionar las omisiones o dilaciones en el cumplimiento de las normas e instrucciones dictadas y a dictarse con relación al problema del año 2000, por parte de las entidades prestadoras del servicio, sin perjuicio de la que recaiga, en forma personal y solidaria sobre quienes ejerzan la conducción de las personas jurídicas cuyas actividades estén

comprendidas en el presente decreto. Que la medida que en el presente se instrumenta, además de responder a las circunstancias de excepción antes descriptas, obedece a razones de urgencia que no permiten aguardar los trámites ordinarios previstos en la CONSTITUCION NACIONAL para la sanción de las leyes tomando en cuenta el carácter perentorio de los plazos comprometidos para afrontar la crisis informática del año 2000.

Art. 3.- Los sujetos comprendidos en la presente norma, deberán obrar con la mayor urgencia, diligencia y pericia en la implementación de los planes de acción que determinen el grado de compatibilidad con el año 2000 de los sistemas aludidos que están a su cargo. *Dicha obligación se extiende a realizar las oportunas acciones tendientes a solucionar la crisis descripta y al diseño e implementación de los pertinentes planes de contingencia para atender los posibles problemas derivados de fallas en los sistemas informáticos y/o equipamientos propios, fallas en las interfases informáticas entre sistemas de información y falta de servicios básicos.* Dichos Planes deberán ser comunicados en igual forma que las declaraciones juradas a que alude el artículo siguiente, dentro de los TREINTA (30) días corridos de publicada la presente medida.

Art. 4.- Los organismos que actúen en la regulación y control de las actividades en las que está comprometido el interés público deberán solicitar a las empresas de los sectores público y privado con ellas vinculadas, dentro del QUINTO (5) día hábil de la publicación del presente, una declaración jurada acerca de la situación actual de los sistemas y dispositivos afectados al servicio que le sea propio, con la expresa mención sobre si se encuentra asegurado el cumplimiento de sus funciones críticas o de la actividad de servicio público cuyo control se verifica en su esfera de competencia. Asimismo les impartirán las pautas sobre las cuales las empresas prestadoras de

servicios públicos deberán desarrollar sus planes de contingencia. Esta información deberá ser suministrada al ente dentro de los TREINTA (30) días corridos de su solicitud, bajo apercibimiento de aplicar multas que oscilarán entre los DIEZ MIL PESOS ($10.000) y los CIEN MIL PESOS ($100.000) por cada día de retardo en la respuesta. Dichas sanciones serán establecidas por acto administrativo, dictado por el ente regulador u órgano de control, según corresponda, y tendrá el carácter de título idóneo para abrir la vía de la ejecución fiscal. El acto administrativo que dispone la sanción puede ser objeto de recurso directo, sin efecto suspensivo, en el término de TRES (3) días por ante la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal de la Capital Federal.

O la aparición de medidas de prevención tendientes a la seguridad física de las personas como está explicito en la Ley:

LEY 24.557

LEY SOBRE RIESGOS DEL TRABAJO

ARTICULO 1 - Normativa aplicable y objetivos de la Ley sobre Riesgos del Trabajo (LRT).

1. La prevención de los riesgos y la reparación de los daños derivados del trabajo se regirán por esta LRT y sus normas reglamentarias.
2. Son objetivos de la Ley sobre Riesgos del Trabajo (LRT):

a) Reducir la siniestralidad laboral a través de la prevención de los riesgos derivados del trabajo;

b) Reparar los daños derivados de accidentes de trabajo y de enfermedades profesionales, incluyendo la rehabilitación del trabajador damnificado;

c) Promover la recalificación y la recolocación de los trabajadores damnificados;

d) Promover la negociación colectiva laboral para la mejora de las medidas de prevención y de las prestaciones reparadoras.

LEYES PROVINCIALES

En la Provincia de San Luis hace tiempo que hay un movimiento general del Gobierno para el crecimiento, avance e inserción de las nuevas tecnologías en todos los niveles. Han sido firmado acuerdos en pos de alcanzar este objetivo, en primer lugar el Acuerdo con la CEPAL, originario del Proyecto SIP (Sistema de Información Provincial) que posteriormente salió a licitación con las Licitaciones 1/99 y 2/99, adjudicadas a Trans S.A. para infraestructura y a Oracle S.A. para aplicativos, en un proyecto que se denominó E-Government, en el cual están enmarcados siete sistemas, soporte de la Intranet de Gobierno, como el Sistema de Mesa de Ayuda y Sistema de Expedientes, a los que se hace mención en varios de las contratos que conforman el programa "Soporte para la intranet de Gobierno – Autopista de la Información" en el cual nos hallamos insertos.

Posteriormente el Gobierno de la Provincia de San Luis encaró un proyecto mucho mas ambicioso y abarcativo, la Autopista de la Información, que prevé la informatización de toda la provincia en todos sus niveles, desde el gobierno como usuario modelo hasta los ciudadanos y empresas privadas.

Dentro de este proyecto se encuadra la generación de políticas de prevención y seguridad, y los planes de contingencia en los que hoy nos encontramos abocados. (Ver marco en Anexo I)

LEY N. 5148

SAN LUIS, 30 de noviembre de 1998

SISTEMA DE INFORMACION PROVINCIAL (CONVENIO)

Art. 1.- En el marco del Convenio firmado entre la CEPAL y el Gobierno de la Provincia de San Luis, ambas Instituciones acuerdan:

OBJETIVOS

1. La asistencia técnica que realizaría la CEPAL a fin de poner en marcha el Sistema de Información Provincial (SIP) tendrá cuatro grandes áreas de acción:
    a) Apoyo a la Dirección Provincial de Informática y telecomunicaciones para la instalación del sistema de comunicación Intra e Internet, de redes locales y equipamiento físico y software de base y de aplicación asociados.
    b) Apoyo a la Dirección de Estadística y Censos en la identificación de otras instituciones públicas incorporables en el SIP y catalogamiento de las fuentes de información existentes y potenciales en cada una. Las estadísticas de recursos humanos (cantidad de empleados, sueldos y salarios, etc.),presupuesto y administración son variables básicas para la elaboración del SIP.

c) Apoyo en la organización de toda la información necesaria: estadística, social, económica, financiera, etc. Generación y desarrollo de banco de datos a partir de la información revelada,

d) Capacitación de personal en cada institución para el mantenimiento y alimentación del SIP, principalmente en las áreas de estadística, administración de redes (locales y de Internet) administración de base de datos y diseño Internet.

2. Como primera etapa de dicha asistencia técnica se efectuará una misión de trabajo in situ para la evaluación del estado actual de los sistemas informáticos,

Art.2 .- El alcance factible del SIP y la formulación de un plan de trabajo elaborado conjuntamente con las contrapartes de la Provincia de San Luis. El plan de trabajo se trabajo se elaborará sobre la base del documento propuesto sobre `Modernización Tecnológica de la Administración Pública Provincial, en particular en lo que concierne a las necesidades de las dos instituciones participantes.

3. El plan de trabajo, con horizonte de un año, especificar :

a) El conjunto de estadísticas que compondrán el esquema básico del Sistema de Información Provincial.

b) La factibilidad de diseñar, instalar y poner en funcionamiento un sistema Internet. además de designar los productos utilizables para la alimentación del sistema dentro de dicho período. La combinación de la red y de los productos de información contenidos en ella constituir el modelo preliminar o experimental del SIP.

c) Un esquema de capacitación de personal de la administración pública para dotar al sistema de los recursos humanos necesarios para su funcionamiento.

d) Un presupuesto tentativo destinado a implementar el modelo preliminar del SIP y una posible fase de expansión, excluyendo el equipamiento.

EJECUCIÓN

El plazo de ejecución de estas actividades ser del 1 de diciembre de 1997 al 31 de diciembre de 1997. Se prevé que algunos funcionarios de la CEPAL viajen a la ciudad de San Luis a fin de plantear el trabajo y discutir los elementos básicos de la metodología propuesta.

El informe final se presentar al finalizar el período establecido de ejecución.

III. PRESUPUESTO

Para contribuir a la realización de estas actividades, el Gobierno de la Provincia de San Luis transferir a la CEPAL a la firma de la presente Acta de Convenio de Cooperación Técnica, la suma de 10.000 (diez mil) pesos argentinos, para cubrir los gastos de consultores asociados, viáticos, pasajes y costos de administración, por todo concepto..

La CEPAL en ningún caso asumir obligaciones que excedan el monto acordado para estas tareas de cooperación. Buenos Aires, 25 de noviembre de 1997

EDGARDO NOYA GRACIELA CORVALAN

ACTA DE CONVENIO DE COOPERACION TECNICA N.2

En el marco de convenio firmado entre el Gobierno de la Provincia de San Luis y la Comisión Económica para América Latina y el Caribe de las Naciones unidas (CEPAL), homologado por Decreto Nro.2955 - HyOP

-SH-97 Del Poder Ejecutivo Provincial, ambas instituciones acuerdan la realización de actividades de cooperación técnica de acuerdo con lo que sigue.

I. MARCO DE REFERENCIA

En apoyo a la modernización tecnológica de la Administración Pública Provincial, el proyecto Sistema de Información Provincial tiene como uno de sus objetivos principales la formulación de un sistema de indicadores socioeconómicos. La ejecución de este proyecto permitir disponer de un amplio conjunto de indicadores de la realidad económica y social de la Provincia, construido con las metodologías más aceptadas nacional e internacionalmente, sistematizado de acuerdo con los requerimientos de las políticas y estrategias llevadas a cabo por el Gobierno de la Provincia, y presentado en forma oportuna de acuerdo con los plazos necesarios para la toma de decisiones. Su ejecución, asimismo, se efectuará en estrecha coordinación del banco de datos que difundir los indicadores seleccionados.

II. OBJETIVO GENERAL

Relevamiento de los indicadores económicos, fiscales y sociales disponibles, evaluación de su representatividad, de las metodologías utilizadas y de la oportunidad de su presentación. Proposición de un conjunto sistematizado de indicadores funcionales a las demandas de política del Gobierno de la Provincia y construcción del sistema de información con las series estadísticas disponibles. Proposición de las actividades necesarias para alcanzar el sistema objetivo de información provincial.

III. ORGANISMO EJECUTOR

El proyecto de Desarrollo del Sistema de Indicadores económico-sociales de la Provincia de San Luis estar a cargo de la Comisión Económica para América Latina y el Caribe de la Organización de las Naciones Unidas (CEPAL).Este organismo prestar la asistencia técnica requerida para el cumplimiento de este proyecto con participación del personal técnico con que cuenta actualmente y con un conjunto de consultores contratados especialmente a tal fin. La coordinación del proyecto estar a cargo del Director de la oficina de CEPAL en Buenos Aires. La Dirección de Estadística y Censo de la Provincia de San Luis constituir la contratapa Provincial.

IV. TAREAS A REALIZAR

El proyecto de referencia se desarrollar en dos etapas. En la primera de ellas, que corresponde a ésta Acta de Convenio N.2, se efectuar una evaluación de los indicadores disponibles y se presentar una propuesta para determinar el conjunto de indicadores marco que integrar el Sistema de Información Provincial. Durante la segunda etapa, que se efectuar mediante la concertación de una nueva acta convenio, se proceder al mejoramiento de los indicadores disponibles y a la construcción de aquellos que se considere de mayor prioridad en el programa de mejoramiento de la estadística básica que se acuerde con la Dirección de Estadística y Censos del Gobierno de la Provincia de San Luis. Los trabajos a realizar durante esta primera etapa serán los siguientes:

1. Consultoría en indicadores económicos.
   a. Se analizar n los principales componentes de la producción de la Provincia, procurando identificar las actividades más relevantes en cada sector económico de origen.

b. Se identificar las prioridades y metas que ha fijado la Provincia en materia de desarrollo económico.

c. Sobre la base de los puntos anteriores, se propondrá un conjunto de variables orientado a fortalecer el sistema de información económica a fin de que permita conocer con oportunidad el estado actual de la situación económica provincial, su evolución histórica, y realizar una tarea de seguimiento sobre su evolución posterior.

2. Consultoría en indicadores fiscales

a. Realizar una actualización de los mecanismos de distribución de los recursos fiscales entre La Nación y las Provincias, particularizando lo referente a la provincia de San Luis.

b. Identificar las prioridades y metas que ha fijado la Provincia respecto de su política fiscal.

c. Realizar un cuadro de la situación fiscal actual de la Provincia donde se expondrán las principales categorías de ingresos y egresos fiscales de la Provincia.

d. Efectuar un inventario del material estadístico disponible.

e. Sobre la base de los puntos anteriores, y como modo de contribuir al seguimiento y análisis de la situación fiscal de la Provincia, propondrá un conjunto de variables e indicadores dirigidos a fortalecer el sistema de información fiscal.

3. Consultoría en indicadores sociales

a. Se elaborará un marco de referencia general para la selección de áreas sociales prioritarias mediante la realización de entrevistas con especial participación de los responsables de las políticas sociales sectoriales.

b. Se identificará, además, las prioridades y metas que ha fijado la provincia en materia de desarrollo social.

c. Se efectuará un inventario de los indicadores disponibles.

Con los resultados anteriores se definir un conjunto de indicadores sociales para cada una de las áreas seleccionadas orientado a fortalecer el sistema de información social de la Provincia.

LEY N. 5152

SAN LUIS, 30 de noviembre de 1998

CYBER PROVINCIA.

Artículo 1:

Aprobar la Carta de Entendimiento, Anexos I y II y el Plan Operativo suscripto por el Gobierno de la Provincia de San Luis, con el Ministro de Industria de Canadá, para el desarrollo de San Luis como Cyber Provincia.

ANEXO A: CARTA DE ENTENDIMIENTO

Art. 1. – Carta de entendimiento

CARTA DE ENTENDIMIENTO

Entre el Gobierno de la Provincia de San Luis, representado en este acto por los señores Ministros Secretarios de Estado de Industria, Turismo, Minería y Producción, Licenciado LUIS BERNARDO LUSQUIÑOS y de Gobierno y Educación, D.HECTOR OMAR TORINO, y el Ministerio de Industria de Canadá, representado en este acto por Sr.MAC PRESCTT, en nombre de la Oficina de Relaciones Internacionales (OIP), Información Highway applicatión Branch (HAB) del Ministerio de Industria de Canadá, en adelante mencionados como las partes:

CONSIDERANDO:

Que en el marco de la política de modernización y actualización del Gobierno de la

Provincia de San Luis, éste tiene como meta desarrollar conjuntamente un sistema interactivo dé para mejorar la calidad de los servicios y fomentar la comunicación con la comunidad y ésta entre sí.

Que el Ministerio de Industria de Canadá juega un rol preponderante en el Gobierno Federal de Canadá en el Desarrollo de Tecnología de Información Telecomunicaciones aplicadas a la enseñanza y servicios comunitarios, coordinando esfuerzos para el beneficio de los ciudadanos de ese país.

Que Canadá es reconocida por estas experiencias en la investigación, desarrollo y provisión de telecomunicaciones, sistemas de enseñanza y otros servicios comunitarios requeridos para las diferentes comunidades..

Que las partes declaran su mutuo interés en la exploración de intercambio de conocimientos y experiencias en la aplicación de tecnologías de información y comunicación en las áreas de enseñanza-aprendizaje y servicios comunitarios, y en el desarrollo conjunto de asesorías en servicios técnicos, tecnológicos y materiales de capacitación.

LAS PARTES SUSCRIBEN:

Cláusula 1: Los objetivos de esta Carta de Entendimiento son explorar el intercambio de experiencias en la aplicación de tecnologías de la comunicación y de la información para el armado de una Red Informática que vincule Complejos Sanitarios, Municipales, Seguridad, Asociaciones No gubernamentales, Red de Escuelas, Empresas y Otros Servicios de la Provincia con el Gobierno Provincial y aquellos entre sí para ello se requiere.

A. Realizar un diagnóstico y relevamiento de necesidades de las unidades provinciales para responder a los desafíos de las nuevas tecnologías de información y la comunicación.

B. Establecer las nuevas formas de acceso a las comunicaciones.

C. Interconectar las unidades institucionales entre ellas y el Gobierno de la Provincia de San Luis.

D. Brindar a los técnicos y profesionales la capacitación necesaria para la utilización y desarrollo de las nuevas tecnologías de la información y la comunicación.

E. Proveer distintas formas de aprovechamiento de la Red Internet.

F. Promover la elaboración de materiales en Castellano para dichas personas.

G. Estimular la participación de miembros de la comunidad y de micro, pequeños y medianos empresarios en proyectos de colaboración y desarrollo conjunto.

Cláusula 2: Las partes manifiestan lo siguiente:

A. Promover el intercambio de información oncernienteva materiales y contenidos para redes, adoptando estrategias para desarrollar en forma conjunta técnicas de instrucción para el uso de las nuevas tecnologías de la información y la comunicación abriendo líneas de investigación para la coprodución y distribución de productos.

B. Trabajando conjuntamente promoviendo en Canadá y en la Argentina el conocimiento y la experiencia derivados de las aplicaciones de la información y la comunicación y el desarrollo comunitario.

C. Evaluará las experiencias canadienses que sean de potencial aplicación a las necesidades argentinas y experiencias que puedan ser compartidas. Se entiende que el Ministerio de Industria de Canadá procurará la participación de terceras organizaciones de su

asociación nacional, para sostener la implementación de esta Carta de Entendimiento y que proveerá las actividades que resulten del presente entendimiento en una combinación de servicios voluntarios y contratados. Se entiende también que el Gobierno de la Provincia de San Luis no se encuentra obligada a la introducción de ninguna tercera parte sin su pleno consentimiento. Esta Carta no será considerada para crear obligaciones legales.

D. Las partes tienen la intención de desarrollar estas acciones mediante Actas Complementarias.

Cláusula 3: Las partes establecerán una colaboración formal para que este presente entendimiento derive en la definición de áreas y modalidades específicas de cooperación incluyendo el nombramiento de un equipo de 3 (tres) representantes de cada una de las partes para el futuro desarrollo e implementación de esta Carta Entendimiento, dentro de los 60 (sesenta) días de la firma de la presente.

Cláusula 4: Cualquiera de las partes puede dar por terminada esta Carta de Entendimiento en cualquier momento, por medio de una notificación escrita a la otra parte con 120 (ciento veinte) días de anticipación debiendo complementarse los compromisos adquiridos.

Cláusula 5: Esta Carta de Entendimiento tendrá una vigencia de 3 (tres) años contados a partir de la fecha. Firmado en 2 (dos) ejemplares de un mismo tenor a un solo efecto en la Ciudad de San Luis, Republica Argentina y en la Ciudad de Ottawa, Canadá, en idioma inglés y castellano, el día 3 de julio de 1998, siendo cada versión igualmente válida por los representantes legalmente autorizados de ambas partes.

ANEXO B: ANEXO A CARTA DE ENTENDIMIENTO

Art. 1.- En el marco de la Carta de Entendimiento suscripta el 3 de julio de mil novecientos noventa y ocho, entre el Ministerio de Industria de Canadá y el Ministerio de Gobierno y Educación de la Provincia de San Luis, en la Localidad de Potrero de los Funes, Provincia de San Luis, República Argentina, a los dieciséis días del mes de septiembre del año mil novecientos noventa y ocho, se reúnen, en representación del Ministerio de Industria de Canadá, el señor MAC PRESCOTT, Director de la Oficina de Acuerdos Internacionales, y el señor HECTOR OMAR TORINO, Ministro de Gobierno y Educación de la Provincia de San Luis, conviniendo la suscripción de la presente acta, y 1 - en virtud que el Gobierno de la Provincia de San Luis tiene la visión de transformar a la misma en la primera ciberprovincia de la Argentina, en función de la experiencia del Gobierno de Canadá y específicamente en varias de sus Provincias ha desarrollado la infraestructura y los procesos para la concreción de las conexiones iterativas de las comunidades. 2 - basado en la coincidencia de buscar el desarrollo tecnológico, social y humano, se acuerda lo siguiente:

B. CONFORMAR un grupo de trabajo integrado por técnicos de San Luis y Canadá, para efectuar el inicio de los términos del prediseño del Plan de Acción que consistiría en los siguientes puntos: -SIP - Sistema de Información Provincial (Intranet de Gobierno)

   A. GOBIERNO ON LINE –

   B. ESCUELAS PUNTANAS EN LINEA –

   C. SISTEMA DE INFORMACION PARA LA PRODUCCION –

   D. CENTRO DE ACCESO COMUNITARIO –

   E. BIBLIOTECAS EN RED –

   F. FORMACION PROFESIONAL Y SU REENTRENAMIENTO LABORAL –

G. DIGITACION DE CONTENIDOS –

H. TELEMEDICINA - HOSPITAL VIRTUAL - HOSPITAL EN RED –

I. RED DE ACCIONES NO GUBERNAMENTALES

B) Las partes convendrán prioritariamente la contratación de expertos canadienses, que asistan y trabajen en forma conjunta con los técnicos de San Luis, en los puntos y temáticas identificados en el presente Anexo.

Los detalles de cada uno serán explicitados en actas complementarias posteriores.

C) La Provincia de San Luis como estado federal, es miembros del Consejo Federal de Inversiones, por lo que hará intervenir a este Consejo, a través de su Programa de Conectividad, en aquellos aspectos cuyo desarrollo tengan coincidencia con los contenidos expresados en este Anexo.

ANEXO AB: ANEXO II a la Carta de Entendimiento firmada el 3 de julio de 1998

Art. 1.- Considerando que: La Provincia de San Luis y el Ministerio de Industria de Canadá han firmado una Carta de Entendimiento el 3 de julio de 1998 con el fin de explorar las oportunidades de cooperación en materia de creación de redes y de aplicaciones para ser utilizadas por la Provincia y por sus ciudades;

Considerando que: La Provincia de San Luis desea establecer alianzas estratégicas que le permitan participar y adquirir pericia en el uso de la tecnología de la comunicación de la información en lo referente al suministro de servicios de red, a la creación e aplicaciones y de servicios para un entorno en línea, y a las estructuras gubernativas y de formulación de políticas correspondientes necesarias;

Considerando que: El Ministerio de Industria de Canadá desempeña un papel primordial dentro del Gobierno Federal de Canadá en el establecimiento de la

estructura de base de la autopista de la información para suministrar servicios gubernamentales, servicios sanitarios y aplicaciones de aprendizaje y para coordinar los esfuerzos nacionales de Canadá con vistas a utilizar la tecnología de la comunicación de información y la tecnología de las telecomunicaciones para el provecho de todos los canadienses;

Considerando que: Las Partes han firmado un Anexo (I) a la Carta de Entendimiento del 3 de julio en el cual se solicita el establecimiento de un equipo de expertos de ambas partes que comience la creación del Plan operacional para hacer de San Luis la primera provincia cibernética de Argentina;

La Oficina de Acuerdos Internacionales del Ministerio de Industria de Canadá, y la Provincia de San Luis en Argentina, han logrado acordar lo siguiente en este Anexo (II):

Artículo 1:

Los objetivos de Anexos son elaborar un Plan operacional que convierta a San Luis en usuario líder y defensor de la tecnología de la comunicación que beneficie social y económicamente a sus ciudadanos. El punto central del estudio lo constituirán las necesidades principales de la Provincia de San Luis entre las que se incluyen: una autopista de la información, sistemas de información provincial, gobierno en línea, redes educativas, sistemas de información para producción, centros de acceso comunitario, bibliotecas

en línea, formación profesional y readaptación laboral, digitalización de contenido, telemedicina y hospitales en línea, y una red de movimientos no gubernamentales.

Las actividades que resulten del Anexo se centrarán en tres áreas específicas:

a) Elaborar de un estudio de vialidad sobre la tecnología de red e I infraestructura,

incluido el análisis de las necesidades, las opciones de tecnología, recomendaciones y el plan de ejecución.

b) Elaboración de un modelo empresarial para el establecimiento de servicios, incluido un plan de acción recomendado que detalle en manera de lograr ventajas económicas para la provincia.

c) Elaboración de recomendaciones relativas a las políticas, al proceso y a la administración de las redes y al suministro de contenido.

Artículo II:

Como consecuencia del acuerdo entre el Ministerio de Industria de Canadá y la Provincia de San Luis, el Ministerio de Industria de Canadá dirigirá y liderará el desarrollo de un Plan Maestro y facilitará las relaciones y mediará entre la Provincia de San Luis y proveedores canadienses especificados con el fin de lograr la elaboración del Plan mencionado. Las partes tienen la intención de que:

a) Internacional Datacastig desarrolle los requisitos del Artículo Ia), reservándose el derecho de subcontratar, según convenga.

b) El Secretariado de la Autopista de la Información de la Provincia de Nuevo Brunswick desarrolle los requisitos del Artículo Ib, reservándose el derecho de subcontratar, según convenga.

c) Lanark Communications Network desarrolle los requisitos del Artículo Ic), reservándose el derecho de subcontratar, según convenga.

d) El Ministerio de Industria de Canadá dirigirá y liderará este proyecto, y continuará ofreciendo su apoyo y su coordinación entre las distintas partes, según convenga.

Artículo III:

Estando de acuerdo la Provincia de San Luis y el Ministerio de Industria con los proveedores canadienses propuestos por el Ministerio de Industria de Canadá arriba mencionados en principio, la Provincia de San Luis contratará los servicios al Ministerio de Industria de Canadá, por un monto total neto de U$S 396,000 (trescientos noventa y seis mil dólares americanos), haciéndose el pago mediante carta de crédito irrevocable en dólares americanos con pagos parciales realizables previo cumplimiento de los objetivos fijados de común acuerdo, y de acuerdo al siguiente detalle.

a) A International Datacasting se le encargará el análisis de las necesidades de infraestructura, la evaluación de las opciones de tecnología, y la elaboración de recomendaciones para la ejecución, pagándosele por ello un honorario neto de U$S 193,0000 - (ciento noventa y tres mil dólares americanos).

b) Al Secretariado de la Autopista de la Información de la Provincia de Nuevo Brunswick se le encargará la elaboración de un modelo empresarial para la puesta en funcionamiento de servicios, incluido el plan de acción para la autopista de la información de San Luis, pagándosele por ello un honorario neto de U$S 80,000.-(ochenta mil dólares americanos).

c) A Lanark Comunications Network se le encargará la elaboración de recomendaciones en materia de políticas, procesos y administración de las redes publicas y en el suministro de contenido público, pagándosele por ello un honorario neto de U$S 93,000.-(noventa y tres mil).

d) Al Ministerio de Industria de Canadá se le encargará la administración del proyecto, pagándosele por ello un honorario neto de U$S 30,000.-(treinta mil dólares americanos)

e) A efectos del presente Anexo, los Planes adjuntos como Apéndices A, representan el plan de trabajo para cada uno de los proveedores identificados en el presente Artículo.

f) El Ministerio de Industria de Canadá subcontratará con los proveedores en la forma que crea conveniente y de la manera que considere apropiada.

g) Los pormenores del presente Anexo se concluirán con la firma de un contrato formal entre el Ministerio de Industria de Canadá y la Provincia de San Luis.

Artículo IV:

a) El objetivo de este documento es únicamente detallar las intenciones de las partes y no crear ningún contrato, sociedad, asociación, organismo u otro tipo de relación que vincule a las partes a cualquier obligación legal.

b) Las Partes podrán, de común acuerdo, introducir enmiendas al Anexo, mediante notificación escrita en la que figure la fecha en la que dichas enmiendas entrarán en vigencia.

c) La terminación de este Anexo no afectará la conclusión de acciones cooperativas formalizadas durante su período de invalidez. Firmado en duplicado en inglés y en español, teniendo ambos textos la misma autenticidad, el 30 de Octubre de 1998 en Fredericton, Nuevo Brunswick, Canadá.

3.3. Análisis

De acuerdo a todo lo expuesto en los puntos 3.1 y 3.2. se puede observar que a nivel Nacional, las normas y reglamentaciones son de nivel general o específicos para el

caso del Año 2000, y no hay una decisión firme en cuanto a encarar este tipo de prevención.

En el ámbito privado (Ver Actividad 1 del contrato "Políticas de Mitigación de Riesgos") se han realizado algunos pasos mas pero tampoco definidos, o por lo menos no se encuadran dentro de todo el ámbito de la organización, se han encontrado planes de contingencia abocados a sectores o áreas críticas, pero no todos los componentes de la organización tienen conocimiento de su existencia o su uso.

En cuanto al Gobierno de la Provincia de San Luis, dentro de todo su proyecto global de la Autopista de la Información, ha encarado con seriedad y firmeza la generación de planes que puedan paliar los riesgos a los que se hayan expuestos los sistemas informáticos y sus componentes en la actualidad.

Por tanto prácticamente no hay normas , leyes o reglas que estén limitando o estandarizando aún las generación de dichos planes y, teniendo en cuenta esto, se realiza una propuesta para encararlos en la Actividad 3 del contrato "Políticas de Mitigación de Riesgos".

4. CONCLUSIÓN

Podemos partir de la premisa que un plan de contingencia es una serie de procedimientos alternativos a la forma de operar "normalmente" de cualquier organización, que se ejecutan en situaciones de riesgos o emergencias.

El plan de contingencia es parte integral de un proyecto, no lo sustituye. La contingencia sólo es aplicable, por su propia naturaleza, por un periodo de tiempo corto y bajo condiciones de emergencia.

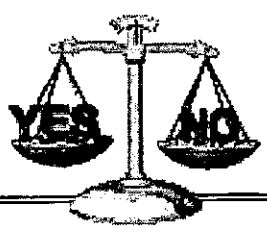
¿Podemos decir que solo afecta a los niveles técnicos?

A primera vista, las contingencias o riesgos parecen conceptualmente sencillos y exclusivamente de carácter técnico. Cuando se analiza con mayor detenimiento, queda claro que, debido a las características y magnitud de cada contingencia, su solución puede ser extremadamente laboriosa y con fuertes repercusiones administrativas y económicas. Es decir, que se debe movilizar una cantidad considerable de recursos físicos y humanos y que se necesita una alta capacidad organizativa para que los equipos puedan estar listos para manejar en forma correcta y eficaz el plan de contingencia adecuado para cada situación.

¿Cuáles pueden ser estos riesgos? Los riesgos pueden ser abarcados desde puntos genéricos y de diferente índole:

- Operativos, ya que los sistemas o algunas máquinas y equipo de proceso con dispositivos inmersos pueden producir resultados erróneos o inclusive dejar de operar, lo que impedirá a las organizaciones atender a sus clientes y usuarios.
- Financieros, por la reducción de sus operaciones y en consecuencia de sus ingresos, así como por el costo de corregir los errores.
- De credibilidad e imagen, sobre todo entre los clientes de la organización que reciban información errónea o no la reciban en absoluto como así también la falta de servicios a usuarios y clientes.

Hay una creencia general de que si la persona no usa PC en ningún ámbito, la contingencia no lo afecta, pero lo cierto es que contingencias graves tienen efectos potenciales sobre toda la población, a



través de la tecnología de la información y los microprocesadores inmersos, que se encuentran en casi todas las esferas de la actividad económica. Su mal funcionamiento puede afectar directa o indirectamente a cualquiera persona, por ejemplo a través de fallas en las telecomunicaciones, suministro de servicios de impuestos,, servicios comunitarios y distribución de alimentos, entre otros.

Actualmente se manejan conceptos que pueden perder significado ubicados fuera de contexto y entonces cabe preguntarse si poseer un plan de contingencia es un reto, una oportunidad o un problema.

Sin lugar a duda es un problema que hay que enfrentar, sin embargo también puede representar una oportunidad, lo que lo transforma en un reto.

Las organizaciones que logren prevenir y evitar mayores conflictos, que puedan anticiparse a un peligro o que puedan detectar a tiempo un riesgo, incluso que puedan paliarlo con los menores costos sociales, políticos y económicos posibles, tendrán ventaja comparativa sobre las que se encuentren rezagadas y más aún sobre las que enfrenten problemas por no haberse preparado para enfrentarlos.

5 . BIBLIOGRAFÍA

Todos los datos de leyes han sido extraídos del Ministerio de Justicia y Derechos Humanos de la Nación – Subsecretaria de Justicia y Asuntos Legislativos – Dirección de Bases de Datos Jurídicas – Sistema Argentino de Informática Jurídica. www.saij.jus.gov.ar

Aclaración: Esta información no es de acceso público, se requiere clave de acceso y password.

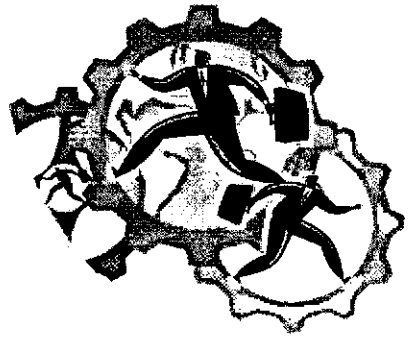
Además se han tomado datos del Boletín Oficial y Judicial de la Provincia de San Luis.

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

ELABORACIÓN DE PLANES DE CONTINGENCIA



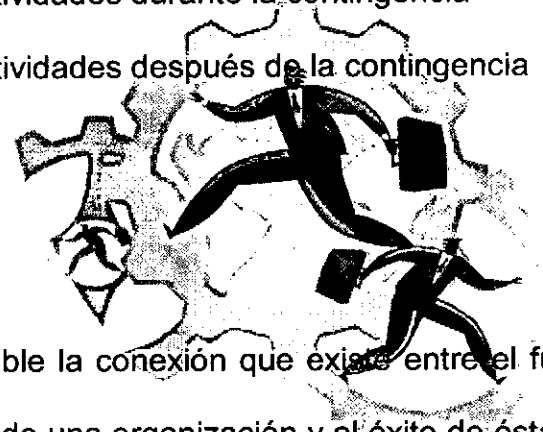
ACTIVIDAD 3

" GENERACIÓN DE PLANES DE CONTINGENCIAS"

"GENERACIÓN DE PLANES DE CONTINGENCIAS"

Índice

1. Enunciado
2. Objetivos
3. Cuerpo
    3.1. Consideración del Riesgo
    3.2 Planes de Contingencias (Software y Hardware)
        3.2.1 Actividades previas a la contingencia
        3.2.2 Actividades durante la contingencia
        3.2.3 Actividades después de la contingencia
4. Conclusión



1. ENUNCIADO

Hoy en día es innegable la conexión que existe entre el funcionamiento eficaz de los recursos informáticos de una organización y el éxito de ésta. Los sistemas informáticos de las organizaciones públicas o privadas son un elemento crítico y es por eso que requieren de una u otra forma protección.

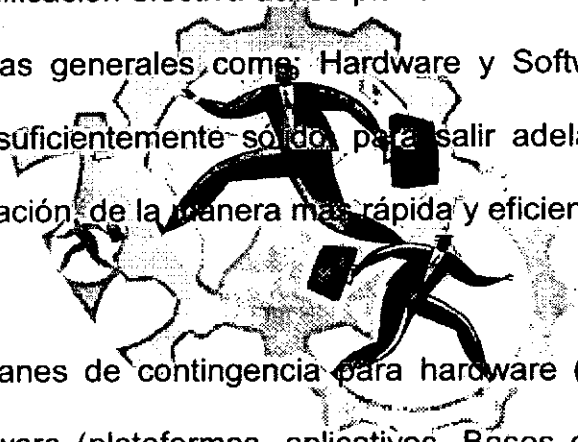
Sin embargo, la protección, por sí misma, no puede ser nunca suficiente. Siempre seguirá existiendo la posibilidad de que ocurra un incidente o contingencia (I/C). Las posibles causas no tienen fin, variando en un rango que va, desde las actividades de un empleado descontento, hasta un incendio generalizado.

Sea cual fuere la causa, las consecuencias son las mismas: la falta de capacidad de una organización para realizar su actividad diaria. Una incapacidad que aumenta día tras día, hora tras hora, hasta que se restaura la actividad normal del Sistema.

La única forma posible de controlar los daños que puede causar un I/C, es planificar detalladamente las reacciones ante cada tipo de contingencia.

La mayor parte de las organizaciones que miran al futuro, tienen Planes de Contingencia que por definición, podemos decir que una contingencia es una situación nunca experimentada previamente por la mayoría de las personas. Planificar una reacción frente a lo desconocido es necesariamente difícil y cuando la I/C sorprende, los planes más sólidos pueden venirse abajo a consecuencia de las tensiones, del pánico o de las improvisaciones.

Es por eso que la planificación efectiva de los planes de contingencias en cada una de sus dos divisiones mas generales como: Hardware y Software, es necesaria para obtener un respaldo suficientemente sólido para salir adelante con las actividades diarias de una organización de la manera mas rápida y eficiente posible.



2. OBJETIVO

Elaboración de los planes de contingencia para hardware (redes, pc's, impresoras, UPS, scanner) y software (plataformas, aplicativos, Bases de Datos y herramientas ofimáticas).

3. CUERPO

Los planes de contingencias abarcan ltodas aquellas áreas, que han sido analizadas en profundidad, mediante un trabajo de equipo, que abarcó los siguientes puntos:

3.1 Consideración del Riesgo

a) Identificación, Declaración y Análisis del Riesgo

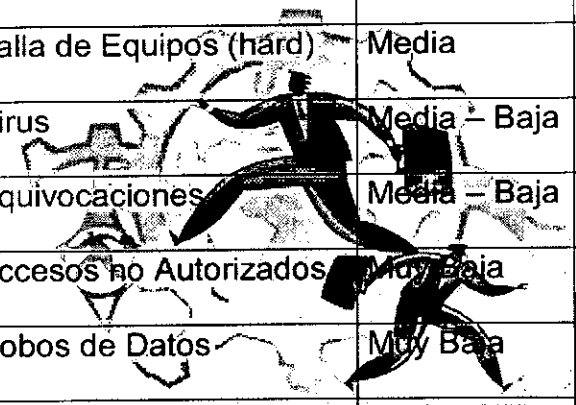
b) Planificación

c) Seguimiento y Control

En estos puntos se mencionarán todos los riesgos que afectan al Área identificada, en donde los riesgos se clasifican según el nivel Usuario o Técnico con el cual se identifiquen para preverlos.

a) Identificación, Declaración y Análisis del Riesgo a nivel Usuario y Técnico.

Grupo afectado	Tipo de Riesgo	Probabilidad del factor	Nivel de Impacto Del (1 al 5)
Ambos	Robo	Muy Baja	Depende de lo extraido
Ambos	Vandalismo	Muy Baja	Depende de lo afectado
Ambos	Falla de Equipos (hard)	Media	4 - 5
Ambos	Virus	Media – Baja	1 - 3
Ambos	Equivocaciones	Media – Baja	1 - 3
Ambos	Accesos no Autorizados	Muy Baja	5
Técnico	Robos de Datos	Muy Baja	5
Técnico	Caída de Servicios en/los Servidores	Media	3 – 5
Técnico	Rotura de Enlace	Baja	5
Ambos	Contaminación*	Media	1 - 3
Técnico	Disparo de Protección Térmica	Baja	5
Técnico	Fallo en caja de Conexión	Baja	5
Técnico	Fallo en los Patch Cord	Baja	5
Técnico	Error de Configuración	Baja	3



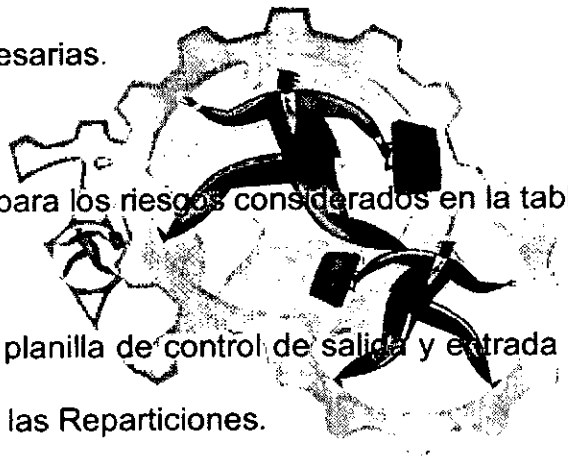
Ambos	Error de Software	Baja	4 - 5
Ambos	Fuego	Muy Bajo	5
Ambos	Fraude	Muy Bajo	5
Ambos	Terremoto	Muy Baja	5

Tabla N° 1

*Contaminantes comunes : polvo, yeso, tierra hollín etc..

Analizando este cuadro podemos observar que los riesgos (marcados con rojo) que tienen impacto y probabilidad media - alta, son los que se deben considerar para generar el Plan de Acción, para el resto de los riesgos se detallaran mas adelante las recomendaciones necesarias.

b) Planificación



Las acciones a tomar para los riesgos considerados en la tabla 1 son las siguientes:

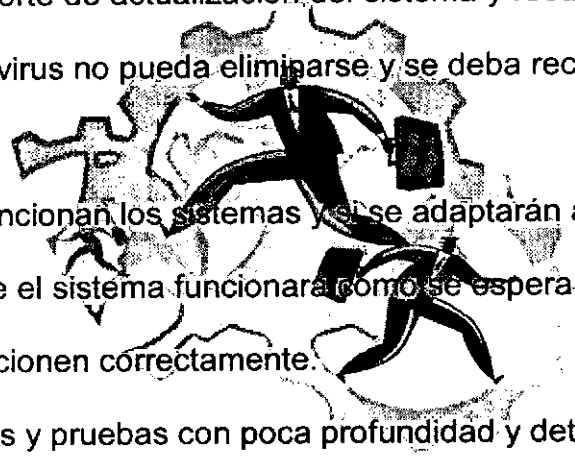
Robo y Vandalismo

- Establecer una planilla de control de salida y entrada del personal con equipos, en cada una de las Reparticiones.
- Tener Identificados a todos y cada uno de los elementos de software y hardware, como así también el personal del área.
- Analizar y establecer la aplicación de las distintas barreras de protección, perimetral, del inmueble, por área y del objeto.
- Colocar fajas de seguridad en los gabinetes para evitar que quiten la tapa del ordenador y se lleven la unidad y tarjetas adaptadoras, placas, etc.
- Complementar y actualizar la seguridad del edificio con las normas aplicadas al área.

Virus

- No instalar programas que no sean originales

- Controlar la entrada de programas con dominio público (*freeware)* y soportados por el usuario o compartidos (*sharware)*. Emplear sólo fuentes fiables para obtenerlos.
- Impedir el acceso a usuarios no autorizados. Establecer empleo de claves de acceso y protector de pantalla.
- Instalar un modulo de protección antivirus actualizable, residente en memoria a nivel de servidor y terminal para los casos que sean necesarios.
- Comprobar con antivirus los ficheros que se traspasen de un equipo a otro.
- Contar con soporte de actualización del sistema y recuperación de datos para el caso en que el virus no pueda eliminarse y se deba reconfigurar el equipo.



Equivocaciones

- Prever como funcionan los sistemas y si se adaptarán a los usuarios.
- No suponer que el sistema funcionara como se espera, sino que asegurarse que los sistema funcionen correctamente.
- Realizar diseños y pruebas con poca profundidad y detenido análisis de estudio.
- Establecer usos y normas de utilización de los sistemas.
- Definir las normas y procedimientos para riesgos de origen humano.

Fallas de Hardware

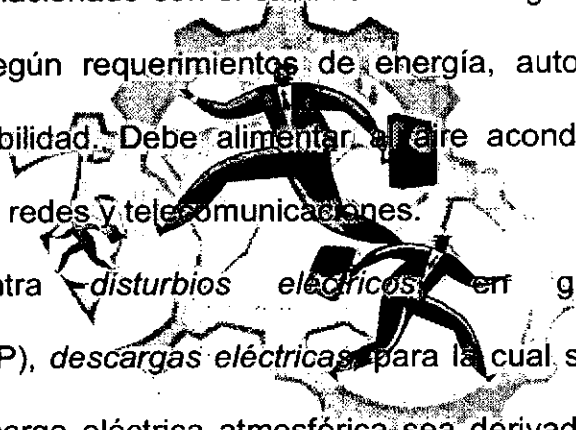
- Definir las normas y procedimientos para riesgos de origen físico.
- Mantener limpio el centro de maquinas o equipos.
- Prohibir fumar comer y beber dentro de la sala de servidores y sobre las PCs personales y otras terminales.
- No instalar purificadores de aire generadores de iones y mantener bien al Aire Acondicionado.
- Asegurar que todos los equipos tengan filtros adecuados.

Caída de Servicios de Servidores

- Monitoreo diario y permanente de los servidores
- Controlar los accesos masivos
- Actualizar las versiones del software utilizado

Las prevenciones para *catástrofes climáticas e incendios* son las mismas a tomar desde el punto de vista de la seguridad edilicia. Deben estar en funcionamiento si el edificio, área u organización en que se encuentra el sistema esta correctamente habilitado, según las normas vigentes.

En cuanto a todo lo relacionado con el *suministro de energía* , se deberá tener UPS y grupo electrógeno, según requerimientos de energía, autonomía, forma de onda, conmutación y confiabilidad. Debe alimentar al aire acondicionado, computadoras, periféricos, equipos de redes y telecomunicaciones.



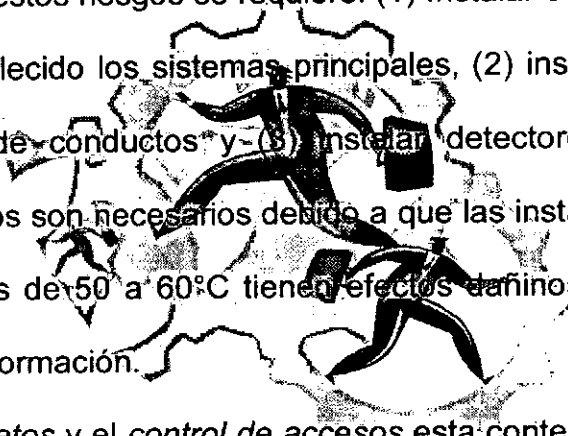
La protección contra *disturbios eléctricos* en general, como pulsos electromagnéticos(EMP), *descargas eléctricas* para la cual se cuenta con pararrayos que hace que la descarga eléctrica atmosférica sea derivada a tierra, disminuyendo además el riesgo de incendio. *Disturbios básicos de trasmisión o de línea*, para lo cual existen supresores de picos, reguladores estabilizadores de voltaje, dispositivos de monitoreo y alarmas.

El control efectuado para el *medio ambiente y contaminación,* que para este caso, es estar conciente de que las partículas dentro del equipo, pueden causar cortocircuitos o incendios. Muchas de estas partículas o contaminantes (polvo, yeso, tierra, hollín y partículas metálicas peligrosas)pueden absorber humedad además de conducir electricidad.

La *humedad*, afecta a los equipos, cintas, discos y papel, por esta razón se considera la instalación de sistemas de detección de fluidos de líquidos al igual que el estudio de

la ubicación del centro de maquinas y equipos por los cuales se tiene especial cuidado con el tema de las cañerías, que no deben pasar por encima, ni debajo, ni a los lados de este centro. Es de fundamental importancia el cuidado a tener con fugas de agua enfriamiento y con los aparatos de Aire Acondicionado (AA) que debe poseer salidas bien distribuidas ya que los problemas ocasionados por los estos implican un doble riesgo: (1) la rotura de AA puede ocasionar que los equipos tengan que ser apagados y (2) las instalaciones de AA son una fuente de incendios frecuente además de ser susceptibles a la instrucción física especialmente a través de los conductos.

- Para poder afrontar estos riesgos se requiere: (1) Instalar equipos de AA de respaldo donde se hayan establecido los sistemas principales, (2) instalar redes de protección en todo el sistema de conductos y (3) instalar detectores de incendios en los conductos.- Los mismos son necesarios debido a que las instalaciones son sensibles a la temperatura, valores de 50 a 60°C tienen efectos dañinos en quipos y medios de almacenamiento de información.



La *protección de los datos* y el *control de accesos* esta contemplado en todo lo que se refiere a políticas de seguridad que se describe en la Actividad 6 del contrato, de acuerdo a una serie de recomendaciones que se deben considerar a la hora en que este plan de seguridad, no resulte y se necesite recurrir a un plan alternativo que es el de contingencia.

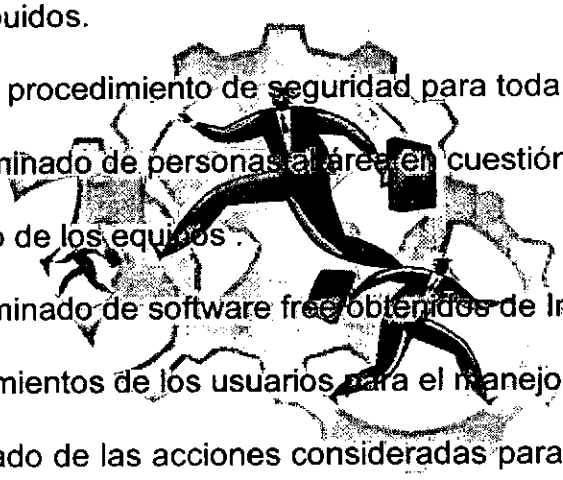
El *software* es un elemento fundamental de nuestros sistemas, la calidad del mismo es un proceso por el cual corresponde asegurar que el software sea desarrollado eficientemente y esté completamente libre de errores y reciba el mantenimiento necesario. También requiere un examen cuidadoso una vez adquirido, antes de ser distribuido en la organización.

c) Seguimiento y Control

Hay que considerar que las acciones a tomar por los riesgos ya priorizados, son de una permanente actualización y vigilancia, es por ello que se identifican a continuación los eventos de activación de estos riesgos para asegurar la funcionalidad de las acciones mencionadas en el punto anterior.

La unidad de medida del riesgo utilizada es de clasificación y de escala como se advirtió en la ***tabla 1*** y los eventos posibles observados de los riesgos considerados son:

- Existencia de objetivos fáciles de robar.
- Sistemas Distribuidos.
- Poco efectivo el procedimiento de seguridad para toda la organización.
- Acceso indiscriminado de personas al área en cuestión.
- Mal uso y abuso de los equipos.
- Manejo indiscriminado de software free obtenidos de Internet.
- Falta de conocimientos de los usuarios para el manejo de equipos informáticos.



Las revisiones del estado de las acciones consideradas para los riesgos se programan de forma regular y para algunos casos se efectúan en los puntos de decisión significativos.

Esto es, realizar controles diarios a todo lo que este relacionado con identificaciones de todo tipo y llevar un registro de las acciones que se hallan definido para cada caso en particular, teniendo en cuenta que coincidan y se relacionen con lo proyectado en el plan de seguridad, para efectuar su correspondiente seguimiento y documentación que se utilizará para elaborar los informes del estado de los riesgos.

El control de los riesgos requiere corresponderse con los procesos de la administración, para corregir las variaciones de los planes en las que lo demande,

respondiendo a los eventos de activación y a su vez , ir mejorando el proceso de la administración de estos riesgos.

3.2. Plan de contingencias

Para realizar los procedimientos de estos planes, se debe garantizar su difusión y estricto cumplimiento.

Los puntos a desarrollar son tres:

3.2.1 Actividades previas a la Contingencia

3.2.2 Actividades durante la Contingencia

3.2.3 Actividades después de la Contingencia

Estos puntos abarcan los dos puntos de vista mas importante; *Software y Hardware.*

3.2.1 Actividades previas a la Contingencia

En esta actividad se desarrolla un plan de acción para establecer o implementar los procedimientos relativos a :

Sistemas de Información:

- *Sistemas Actualmente Funcionando*: Operativos: Unix – Windows Server
- *Aplicativos*: e-government (Mesa de Ayuda – Portal del empleado – Sistema de Expedientes – Sistema Contable – etc.)
- *Lenguaje o paquete con el que fue creado el sistema*: Oracle
- *Gerencia a Cargo:* Secretaria de Estado de Tecnologías de la Información
- *Las unidades o departamentos que usan la información*: Toda el área del poder ejecutivo provincial.
- *Volumen de los archivos que trabaja el sistema:* El volumen es muy grande dependiendo de los aplicativos y de la información que se manipula por medio de Internet. Esto da a considerar la importancia de los datos y su seguridad.

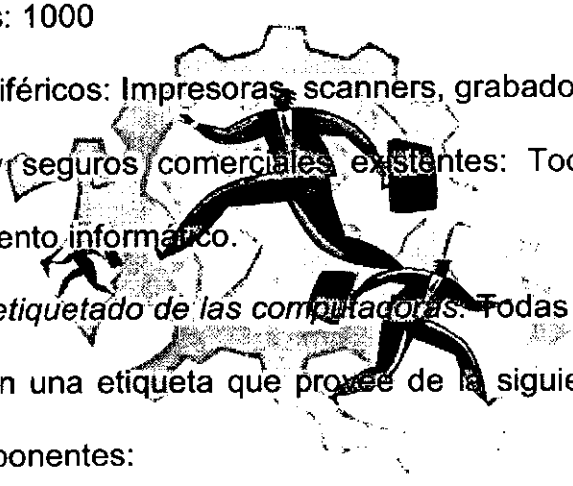
- *Volumen de transacciones diarias, semanales y mensuales que maneja el sistema:* Alto e imprescindible su realización.
- *Nivel estimado en que la Organización pueda funcionar , sin disponer de la información del sistema:* No se puede llegar a un nivel estimado debido a que la baja total del sistema seria critico, no así la parcial, aunque en este caso el nivel estimado es muy bajo.
- *Equipos Informáticos:*

  Servidores: 12

  Maquinas: 1000

  Otros periféricos: Impresoras, scanners, grabadoras, etc

  Pólizas y seguros comerciales existentes: Todos aquellos referidos a equipamiento informático.



- *Señalización o etiquetado de las computadoras:* Todas los equipo se encuentran identificados con una etiqueta que provee de la siguiente información de cada uno de los componentes:

  Nro. De orden

  Nro. De Serie

  Modelo

  Área a la que pertenece

  Características principales

- *Las maquinas fijadas como requeridas para el funcionamiento correcto del sistema:* Los servidores
- *Procedimientos de Backup utilizados* :Los procedimientos de Backups son aquellos que utilizan la metodología presentada en el proyecto "Soporte para un

San Luis Conectado" Actividad 15 "Metodología para el resguardo de datos" la cual se adapto según las necesidades de los sistemas y/o aplicativos.

- *Las políticas utilizadas* : Las políticas a seguir e incorporar son aquellas sugeridas en la Actividad 6 "Planes y Políticas de Seguridad del Contrato "Mitigación de Riesgos" .

En este punto es importante señalar que la información proporcionada es limitada, debido a normas de seguridad en cuanto a información publicada.

Formación de Equipos operativos

Las personas designadas como responsables de la seguridad de la información en las áreas tales como Servidores, Aplicativos, Base de Datos, Parque Informatico, Internet, redes, etc. serán los jefes o encargados de dichas áreas, los cuales deberán generar procedimientos de seguridad para dejar constancia por escrito, además de realizar la Concientización y conocimiento a toda la repartición y organización.

El responsable realizará comprobaciones puntuales para asegurar que las copias de seguridad se realicen según el plan aprobado, para algunas de las áreas mencionadas encontramos estos procedimientos detallados en los contratos afectados del CFI referidos a seguridad y resguardo de la información.

El responsable de la seguridad física e inmueble del edificio es el personal de mantenimiento.

Formación de Equipos de Evaluación

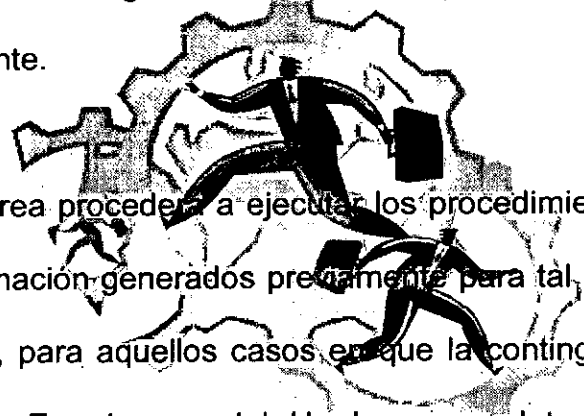
En este punto se determina se analiza si la mejor opción es contratar personal externo para realizar el seguimiento de control en el cumplimiento de los procedimientos de seguridad.

También es importante que la gerencia internamente realice su propia intervención por medio de auditorias periódicas a las áreas, por ellas afectadas.

Los auditores internos y el personal de seguridad destinados a tal fin, deben revisar que se les de una adecuada protección a los datos. Debido a que ellos no tienen control físico sobre esto, no pueden tener la responsabilidad principal de su cuidado, pero si del cumplimiento de las normas y procedimientos de seguridad. Las normas se han de trasladar en la jerarquía para las acciones adicionales necesarias.

3.2.2. Actividades Durante la Contingencia

Una vez presentada la contingencia, se deberán ejecutar las siguientes actividades, planificadas previamente.



Plan de Emergencias

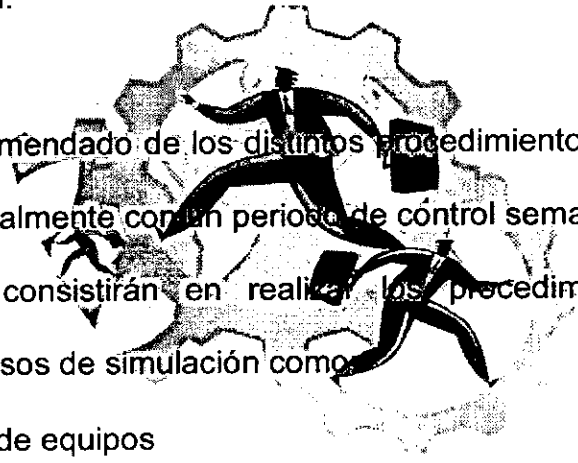
En este punto cada área procederá a ejecutar los procedimientos para la seguridad y resguardo de la información generados previamente para tal acontecimiento junto con la difusión del mismo, para aquellos casos en que la contingencia solo haya sido de software o hardware. En el caso del Hardware se determinará, si fue rotura o desperfecto y a quien se le debe adjudicar la responsabilidad, utilizando para el ello las garantías o seguros correspondientes

El grupo de mantenimiento deberá ejecutar sus procedimientos de resguardo o recaudo si la contingencia o siniestro lo posibilitan de los activos de la organización, teniendo en cuenta; las mejores vías de Salida o Escape de la organización y del edificio, el plan de evacuación del personal presente, las secuencia de llamadas a realizar (policía, bomberos, etc.), la ubicación y señalización de los elementos contra siniestros (extinguidotes, cobertores de agua, etc).

Formación de Equipos

La formación de los equipos estarán establecidas por escrito con los datos personales necesarios para su ubicación e identificación además de contener el detalle de las funciones a desarrollar por cada uno.

Esta información no se pública debido a que es inconsistente para el informe los datos de estas personas, ya que estos pueden variar con la rotación o cambio de personal del área, quedando definido como jefe de seguridad, cada uno de los jefes de área mencionado anteriormente, quienes son los encargados de establecer también las funciones a cubrir por su personal a cargo, según los planes de seguridad elaborados por el área en cuestión.



Entrenamiento

El entrenamiento recomendado de los distintos procedimientos a seguir será realizado en profundidad mensualmente con un periodo de control semanal.

Los entrenamientos consistirán en realizar los procedimientos de seguridad y emergencias en los casos de simulación como:

- Faltante de equipos
- Infección de virus en el sistema
- Corte de energía
- Corte de servicios de red y servidores
- Fuego
- Evacuación del personal
- Salva taje de activos y equipos

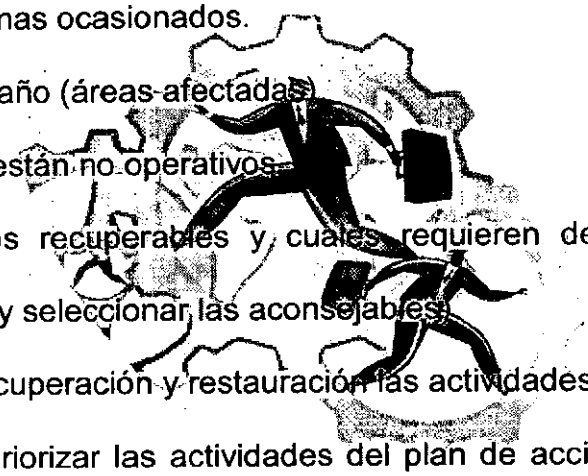
Con estas simulaciones se busca obtener del personal :

- Conocimiento claro de las funciones para un caso real de contingencia
- Conciencia en la prevención y uso de los sistemas y equipos

- Control de la situación
- Determinar los tiempos de realización de estos procesos
- Observar el comportamiento del sistema y tiempo de recuperación y backups
- Experiencia de uso de los equipos de emergencias. Ej. Extinguidores
- Puntos descubiertos o no previstos (que luego deberán ser previstos)

3.2.3 Actividades después de la contingencia

En esta parte de la actividad se realiza un informe de los equipos y sistemas afectados detallando los problemas ocasionados.



- Magnitud del daño (áreas afectadas)
- Sistemas que están no operativos
- Cuales son los recuperables y cuales requieren de soluciones alternativas (mencionarlas y seleccionar las aconsejables)
- Tiempos de recuperación y restauración las actividades o procesos, etc.

Lugo se procede a priorizar las actividades del plan de acción, para llevar a cabo la ejecución de las mismas, en un informe de avance de los trabajos recuperados y de los inconvenientes que pudieran llegar a surgir, para ser entregados a los superiores involucrados.

Una vez finalizada las tareas de recuperación se procede a evaluar los resultados de nuestro plan de acción y seguridad ejecutado, evaluando objetivamente:

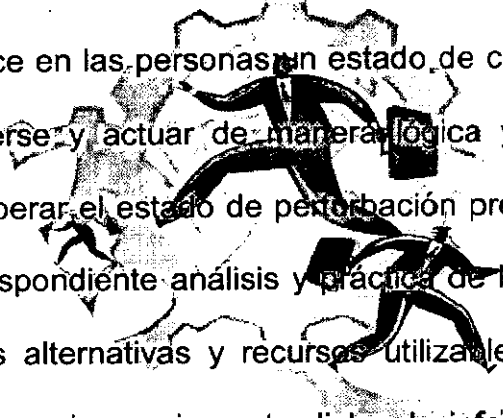
- Personal
- Procedimiento o actividades desarrolladas para la recuperación.
- Circunstancias a favor y en contra presentados.
- Tiempo utilizado

De ellas se obtendrá las recomendaciones y retroalimentación para nuestro plan de acción.

4. CONCLUSIÓN

Para enfrentar una situación límite se tiene que prever planes de contingencias y adoptarlos conjuntamente.

Ante la presencia ineludible de riesgos en cualquier actividad laboral, es indispensable saber cómo debe actuar cada organización según la gravedad de los casos. Para eso, hay que comprender el concepto de contingencia, adoptar distintos planes para enfrentarla y trabajar en forma mancomunada.



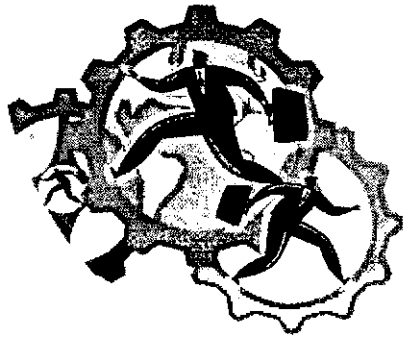
Esta situación, produce en las personas un estado de conmoción (shock), del cual se hace difícil sobreponerse y actuar de manera lógica y organizada. Sólo se podrá afrontar y tratar de superar el estado de perturbación presentado, si se ha previsto tal situación, con el correspondiente análisis y práctica de las acciones a realizar, en las que se encuadren las alternativas y recursos utilizables. De manera tal que en el momento de la contingencia propiamente dicha, la información esté tan incorporada que no sea necesario pensar y se pueda actuar automáticamente. Pero para llegar a esta instancia hay que contar con estos Planes. Es decir, no basta con buenas intenciones. Es necesario prepararse, tomar conciencia, organizarse. Si ello no ocurre, la alternativa no es otra que asumir el riesgo.

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

ELABORACIÓN DE PLANES DE CONTINGENCIA



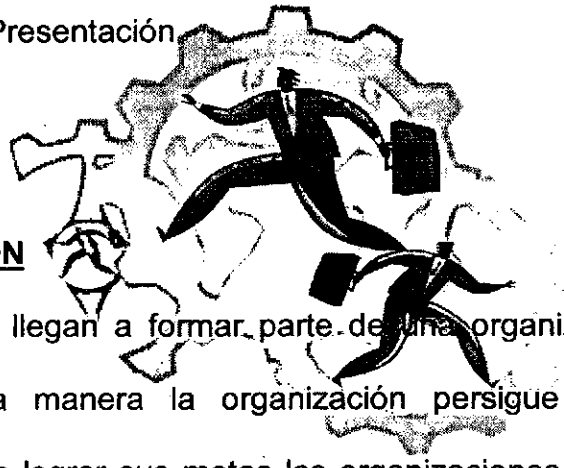
ACTIVIDAD 4

"CONCIENTIZACIÓN Y CAPACITACIÓN EN PLANES DE CONTINGENCIA"

CAPACITACIÓN Y CONCIENTIZACION EN PLANES DE CONTINGENCIAS

Índice

1. Introducción
2. Objetivos
3. Cuerpo
   3.1 Concepto de Concientización
   3.2 Material de Capacitación
   3.3 Seminario – Contenidos
   3.4 Filminas – Presentación
4. Conclusión



1. INTRODUCCIÓN

Cuando las personas llegan a formar parte de una organización llevan sus propias metas, de la misma manera la organización persigue sus metas y objetivos organizacionales. Para lograr sus metas las organizaciones necesitan a las personas de la misma forma que éstas requieren de las organizaciones para satisfacer sus metas individuales. El interés de ambas partes debe encontrar un punto de coincidencia, convertirse en un interés mutuo donde ambos ganen a través de las metas superiores que se generen con la integración de personas y organización.

Este es el camino para iniciar la concientización de las personas que pertenecen a la Organización (en nuestro caso la Administración Pública Provincial), lograr unificar las metas de ambos grupos, para que la organización transmita sus metas a corto, mediano y largo plazo, se prepara este seminario de concientización. El fin es que toda la APP se encamine detrás de los objetivos de la organización en su conjunto.

Asimismo el comportamiento de las personas siempre obedece a la motivación por satisfacer sus necesidades. Es necesario descubrir esa motivación, capacitar forma parte de este importante proceso, ahora bien, las personas se motivan no por lo que piensan que deben hacer o tener, sino por lo que en verdad desean o necesitan; material, emocional o espiritualmente.

Por lo tanto capacitación y concientización van de la mano, comúnmente se dice que capacitar es enseñar, es dar conocimiento, poner a la persona en conocimiento de algo nuevo y concienciar es "ponerle la camiseta", que tome conciencia de que es necesario realizar ciertas tareas para beneficio de la Organización y para su propio beneficio.

Con este pensamiento como base es que se realizará un seminario de concientización, en filminas y la organización básica de las pautas a seguir para capacitar a la APP en los planes de contingencia desarrollado en las actividades precedente contrato.

2. OBJETIVO

Armado de contenidos de un seminario de capacitación y concientización en el uso de la herramientas generadas en el punto precedente (Actividad 3) a fin de poder anticiparse, mediante la difusión masiva, en tiempo y forma de las contingencias que puedan presentarse.

El mismo será entregado a la gerencia de concientización comunitaria para que sean ellos los encargados del dictado del mismo.

3. CUERPO

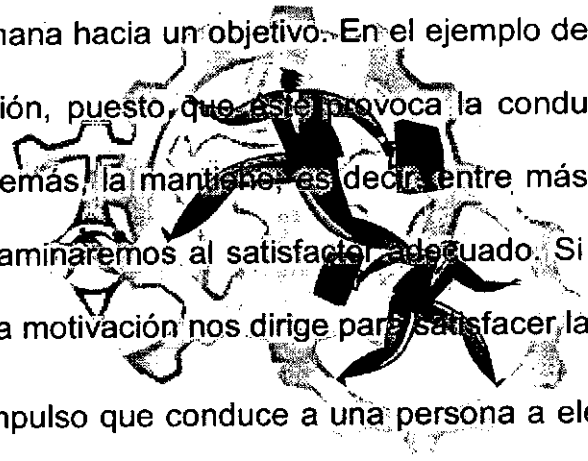
3.1 Concepto de Concienciación

Cuando pensamos en el concepto CONCIENTIZACION parecería que todo es claro y evidente. Si decimos "concientización", se refiere simplemente a "tomar conciencia" de algo. Y seguramente una verdad como esta no necesita una conferencia, ni siquiera una discusión.

La concientización, que encaramos en lo que es Contingencias en la tecnología de la Información, es un concepto mucho más amplio, que no solo abarca el "tomar conciencia" sino también "tomar acciones". Es por ello que ante la posibilidad de que ocurra un incidente, hay que realizar las acciones necesarias para evitar que este se lleve a cabo, estas acciones resultan tomando conciencia de la existencia del problema y lo que este implica.

A esto se lo denomina "la acción de la concientización" y esta nace de la motivación de la persona.

La motivación está constituida por todos los factores capaces de provocar, mantener y dirigir la conducta humana hacia un objetivo. En el ejemplo del hambre, evidentemente tenemos una motivación, puesto que ésta provoca la conducta que consiste en ir a buscar alimento y, además, la mantiene; es decir, entre más hambre tengamos, más directamente nos encaminaremos al satisfactor adecuado. Si tenemos hambre vamos al alimento; es decir, la motivación nos dirige para satisfacer la necesidad.



La motivación es el impulso que conduce a una persona a elegir y realizar una acción entre aquellas alternativas que se presentan en una determinada situación; está relacionada con el impulso, porque éste provee eficacia al esfuerzo colectivo orientado a conseguir los objetivos de la organización, por ejemplo, y empuja al individuo a la búsqueda continua de mejores situaciones a fin de realizarse profesional y personalmente, integrándolo así en la comunidad donde su acción cobra significado.

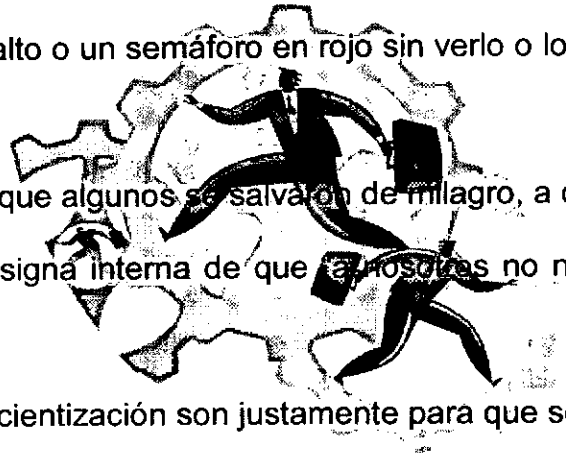
La motivación es a la vez objetivo y acción. Sentirse motivado significa identificarse con el fin. La motivación es resultado de la interacción del individuo con la situación.

Es así como la motivación se convierte en un elemento importante, entre otros, que permitirán canalizar el esfuerzo, la energía y la conducta en general del trabajador hacia el logro de objetivos que interesan a las organizaciones y a la misma persona.

Por esta razón, es importante concientizar para lograr la motivación necesaria de los recursos humanos a fin de alcanzar las metas organizacionales.

¿Cómo nos sirve todo esto en el tema de evitar llegar a una contingencia en el área tecnológica?

Obviamente, si no conocemos un peligro, será muy difícil tenerlo en mente. Sin embargo, la mayoría de las personas que conducen una automóvil sabe que pasar velozmente una intersección cuando se supone que hay que detenerse puede fácilmente ser la causa de serias lesiones. Aún así, 90 por ciento de las personas a las que se les pregunta si lo había hecho dijo que habían hecho justo eso, se habían pasado una señal de alto o un semáforo en rojo sin verlo o lo vió demasiado tarde para hacer algo.



Somos concientes de que algunos se salvaron de milagro, a otros les fue peor.

Siempre existe la consigna interna de que "a nosotros no nos va a pasar" hasta que nos sucede.

Las campañas de concientización son justamente para que se tome conciencia,

y se conozcan las consecuencias que puede acarrear no prestar atención a la señal de peligro.

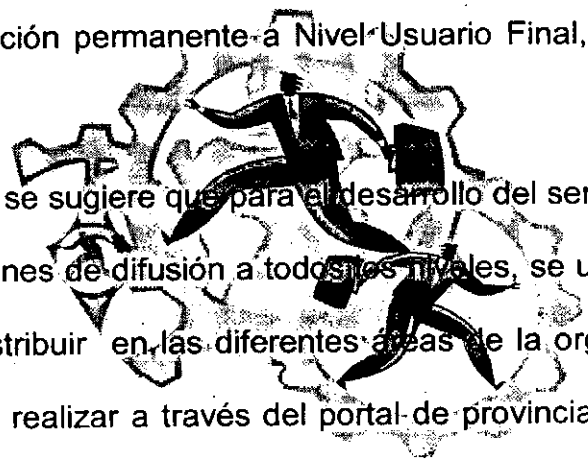
Los mismo sucede con los equipos informáticos. El 90% de la gente no realiza copias de seguridad y cuando se rompe un disco rígido o se corta la luz en medio de un extenso trabajo llegan las lamentaciones "si lo hubiera sabido" pero ya es muy tarde.

Por esto en el desarrollo de todo el contrato "Políticas de Mitigación de Riesgos" se han analizado los puntos de Medidas de seguridad y Planes de Contingencia y en función de los mismos se arma un seminario orientado a capacitar y concientizar a la APP para que se tomen los recaudos necesarios y aún llegado al incidente sepan como deben reaccionar.

3.2. Material de Capacitación

El éxito de un plan de contingencia, se basa en el adecuado conocimiento de los elementos necesarios para llevarlo adelante, por parte de todos los integrantes de la organización. Desde aquellos que ocupan los escalones más altos de decisión, pasando por quienes tienen responsabilidades intermedias, hasta el último nivel de ejecución con influencia directa o indirecta en la calidad, necesitando manejar las técnicas y herramientas adecuadas para su función.

Para que la eficiencia y prevención sea exitosa, la formación y actualización debe ser un tema de preocupación permanente a Nivel Usuario Final, Referente Informático y Nivel Gerencial.



En cuanto al material, se sugiere que para el desarrollo del seminario de capacitación y concientización con fines de difusión a todos los niveles, se utilicen afiches y folletería (ver Anexo I) para distribuir en las diferentes áreas de la organización. La difusión y actualización se debe realizar a través del portal de provincia, correo electrónico, etc. además de proponer invitaciones individuales a los superiores de cada una de las áreas a fin de crear también por este medio conciencia de lo importante que es la capacitación y concientización en los distintos niveles jerárquicos y evitar de esta forma todo tipo de inconvenientes informáticos en cualquier punto de la rama organizacional.

El material a entregar y a exponer propuesto para los concertantes para los distintos niveles serán los siguientes:

A. Guías y resúmenes para el participante

Este material consiste en:

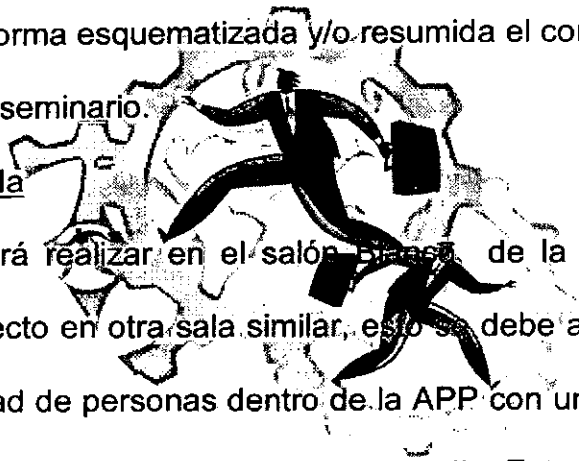
- Para el caso del usuario final en puntos que se trataran en el seminario con una breve explicación.

- Para el informatico se dará una guía basada en el esquema a seguir para realizar planes de contingencias
- Para el Nivel Gerencial se le entregara los puntos principales a considerar que cubren los objetivo de una concientización en la implementación de Planes de Contingencias y funciones que deben fijarse para llevar a cabo esta planificación junto a su personal dentro de la organización.

B. Apoyo con material audiovisual (transparencias)

El material audiovisual utilizado esta basado en un conjunto de filminas, que serán presentadas mediante un proyector dedicado para tal fin.

Estas contendrán en forma esquematizada y/o resumida el contenido de los puntos principales del seminario.



C. Un sala dedicada

El seminario se deberá realizar en el salón Blanco de la casa de Gobierno de la Provincia o en su defecto en otra sala similar, esto se debe a la necesidad de llegar a cubrir la mayor cantidad de personas dentro de la APP con un periodo de duración, no mayor a 3hs. con un descanso de 20 minutos en medio. Este seminario se realizara en 4 presentaciones durante dos semanas consecutivas, lo mismo se aplica al caso de los Referentes Informáticos y el Nivel gerencial, es decir que dependiendo del nivel a quien se le dará el seminario se realizarán las presentaciones, una vez terminado un nivel se procederá a comenzar con el siguiente.

D. Ejemplos prácticos, cuestionarios, etc

Para los distintos niveles en cada una de las guías al final estarán nombrados alguno de los ejemplos a citar por el seminarista al igual que un breve cuestionario o practico en su defecto, con el que se obtendrá el nivel del grupo y del dictado del seminario

pudiendo distinguir los puntos flojos, los cuales una vez aclarados deberán ser reforzados para la próxima presentación.

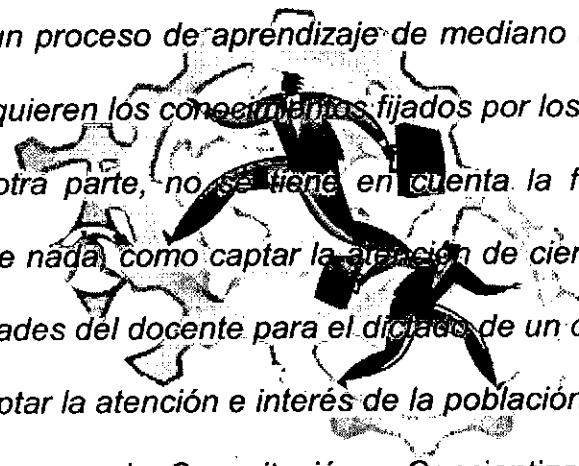
E. Muestra de equipos de emergencias

Las muestras de los equipos de emergencia consiste en conseguir para la exposición, un mata fuegos y explicar su uso, los carteles de las señalización usada en caso de emergencias y su aplicación y demás materiales que aporten para su conocimiento.

3.3. Seminario

El seminarista realizará una introducción de lo que significa concientización y para que sirve la capacitación.

"La capacitación es un proceso de aprendizaje de mediano a corto plazo mediante el cual, las personas adquieren los conocimientos fijados por los objetivos definidos. En la concientización, por otra parte, no se tiene en cuenta la forma de educar o como enseñar, sino mas que nada, como captar la atención de cierta clase de gente. No se consideran las habilidades del docente para el dictado de un curso, sino las habilidades del diseñador para captar la atención e interés de la población con la campaña".



Ver "Pautas Generales para la Capacitación y Concientización" Actividad N° 7 dell contrato *"Políticas de Mitigación de Riesgos"*.

Es importante que el usuario sepa identificar cual es el fin que se persigue con esas dos consignas para así poder iniciar el tema que nos compete.

Las siguientes guías son las que se le entregaran a los oyentes de los distintos niveles.

Guía del Seminario para el Usuario

En este seminario trataremos los siguientes puntos:

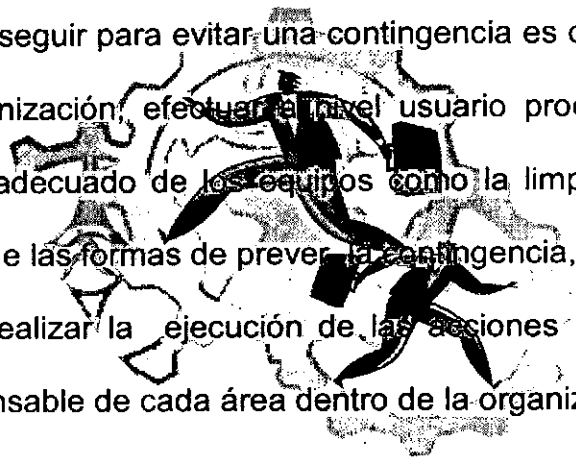
Punto 1: La Contingencia y la importancia de establecer un plan para preverla.

Una **Contingencia** es un ataque o amenaza que pueda sufrir la organización o sector de trabajo de manera impredecible.

Un **Plan de contingencia** es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. *Los planes de contingencia también se conocen como planes de continuidad.*

Punto 2: Procedimientos y/o actividades a desarrollar para evitar una contingencia o incidente.

Los procedimientos a seguir para evitar una contingencia es cumplir con la políticas de seguridad de la organización, efectuar a nivel usuario procedimientos de backups, considerando el uso adecuado de los equipos como la limpieza y buen trato de los mismos, esta es una de las formas de prever la contingencia, y en caso de que esta se presente se deberá realizar la ejecución de las acciones previstas por el personal especializado y responsable de cada área dentro de la organización.



Punto 3: Efectos y documentación a considerar luego de una contingencia

Una vez concluida la contingencia, el usuario final debe, para el caso en que su lugar de trabajo no hubiera sido afectado físicamente, revisar su equipo de trabajo y comenzar por restaurar su información desde backups u otros equipos donde haya resguardo su ambiente de trabajo.

EJEMPLO DE SITUACIONES DE EMERGENCIA

- Incendio

En este caso el procedimiento típico sería abandonar el lugar guiados por las señales de salidas de emergencia.

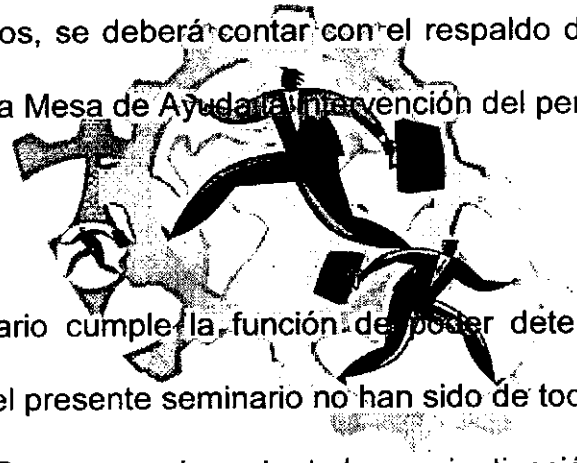
Obedeciendo a el personal a cargo de la situación, el cual estará capacitado para resolver el inconveniente.

- Caída general de la RED

Se solicitará información de los pasos a seguir a la Mesa de ayuda para que esta de comunicado al área correspondiente del incidente, esperando la confirmación del equipo técnico para su posterior informe y solución.

- Error de Hard en los equipos

Para este tipo de casos, se deberá contar con el respaldo de backups del equipo en cuestión, y solicitar a la Mesa de Ayuda la intervención del personal técnico.



CUESTIONARIO

El siguiente cuestionario cumple la función de poder determinar si algunos de los puntos expuestos en el presente seminario no han sido de todo claros.

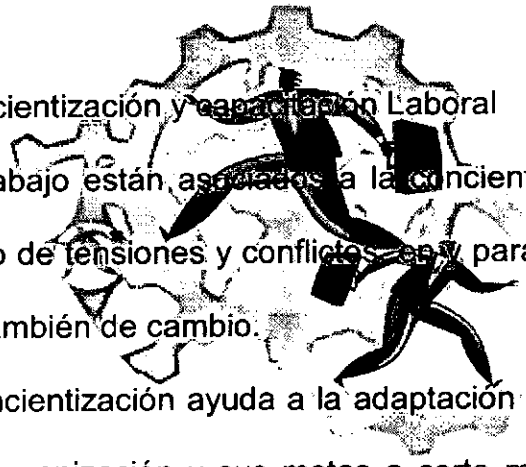
1- ¿Cree que es importante la concientización de contingencias?
2- ¿Puede Ud. identificar una amenaza dentro de su ambiente de trabajo?
3- ¿De que formas Ud. realizaría resguardo de su información?.
4- ¿Cuales son las acciones que Ud. ejecutaría en caso de sufrir algún imprevisto técnico en su equipo de trabajo?
5- ¿Ud. tenía conocimiento de los procedimientos existentes ante una emergencia física?

De esta forma se muestra el uso que tiene en la APP la Mesa de Ayuda "Help Desk" pieza fundamental de comunicación y ayuda al usuario en todos sus niveles. Para descripción de sus niveles, objetivos y funcionamiento ver la actividad 8 del contrato *"Políticas de Mitigación de Riesgos"*

Hay referencias también en Actividad 6 Políticas de Seguridad de Alcance General del contrato *"Políticas de Mitigación de Riesgos"*

Guía del Seminario para el Nivel Gerencial

Los puntos que trataremos en este seminario son:



Punto 1: Cambio, concientización y capacitación Laboral

La producción y el trabajo están asociados a la concientización y capacitación. Esta relación ha sido objeto de tensiones y conflictos en y para el trabajo como un proceso de adaptación, pero también de cambio.

La capacitación y Concientización ayuda a la adaptación o al cambio en la medida en que colabore con la organización y sus metas a corto mediano y largo plazo. Es un proceso de convertirla en una organización inteligente, que requiere de usuarios que aprenden en un contexto complejo y de constante cambio, así es como la motivación se convierte en un elemento importante de la concientización de los empleados entre otros....

Punto 2: La importancia de la concientización de prevenirse ante una contingencia.

Este punto trata de mostrar un poco el equipo informatico, contenido, funciones, etc. con el que cuenta la organización, su importancia de modo que de ser rescatados en la

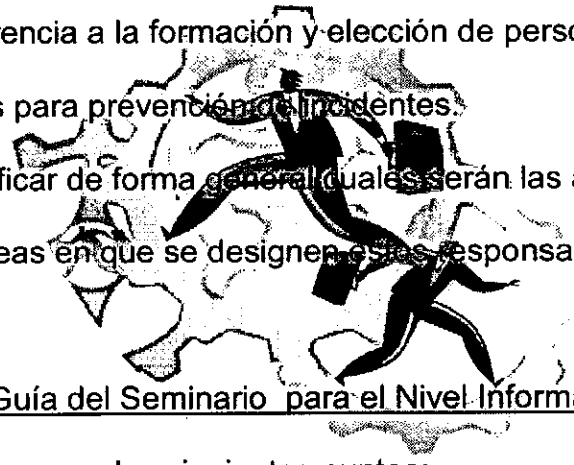
medida de que la información se recupere sigan en funcionamiento ante cualquier eventualidad superior a las esperadas.

El reconocimiento de que la información es un activo valioso para la organización, es un proceso difícil. Aceptamos como una realidad que los datos están disponibles, son confiables y están protegidos de divulgación indebida, sin ver el nivel de dependencia que la organización puede tener de esos datos hasta que los mismos faltan o son afectados de algún modo...

Punto 3: Equipos Operativos – Actividades a Cargo

Este punto hace referencia a la formación y elección de personas que llevan a cabo el Plan de Contingencias para prevención de incidentes.

Podremos ver e identificar de forma general cuales serán las actividades a desarrollar en cada una de las áreas en que se designen estos responsables.



Guía del Seminario para el Nivel Informatico

En este seminario trataremos los siguientes puntos:

Punto 1: La Contingencia y la importancia de establecer un plan para preverla.

Una **Contingencia** es un ataque o amenaza que pueda sufrir la organización o sector de trabajo de manera impredecible.

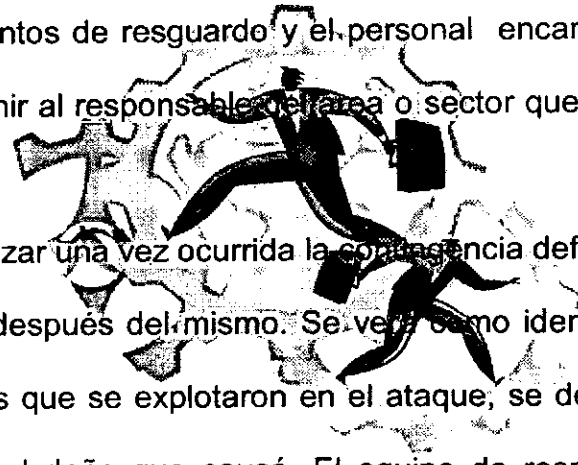
Un **Plan de contingencia** es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. *Los planes de contingencia también se conocen como planes de continuidad.*

Punto 2: El Riesgo - Valoración del Riesgo

La base de un plan de Contingencia radica en la realización de un **análisis de riesgos** en el cual veremos, que implica el examen de cada uno de ellos y su clasificación por niveles, a partir de la probabilidad de su ocurrencia y la severidad del impacto que puedan producir e incluye la toma de decisiones sobre la base de criterios de costo-beneficio con relación a las medidas a implementar para la protección de los activos.

Punto 3: Actividades a desarrollar Antes, Durante y Después de una Contingencia.

Para estar preparados antes de una contingencia o incidente, se debe establecer un Plan de Acción en el cual se verá el tema del stock de la organización por área, las políticas y procedimientos de resguardo y el personal encargado en ejecutar el plan. Además se debe definir al responsable del área o sector que se encuentren dentro de la organización.



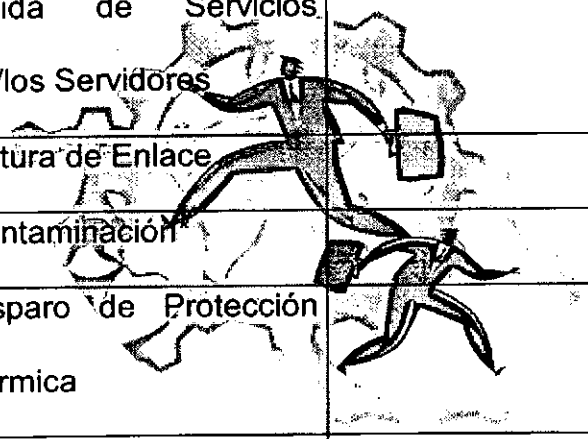
Las actividades a realizar una vez ocurrida la contingencia definen los pasos que deben adoptarse durante o después del mismo. Se verá como identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, se deberá determinar por qué tuvo lugar, y reparar el daño que causó. El equipo de respuesta a incidentes debe incluirse en los pasos adoptados durante o después del ataque para ayudar a evaluarlo, a documentar el evento y a aprender de él.

PRACTICA - EJEMPLO

1) La siguiente tabla se usará a modo de ejemplo para realizar la identificación del riesgo estableciendo la probabilidad de que ocurra y determinar que nivel es el afectado (Usuario y Técnico).

El factor de probabilidad se mediara en (bajo – medio – alto)

GRUPO AFECTADO	TIPO DE RIESGO	PROBABILIDAD DEL FACTOR	NIVEL DE IMPACTO DEL (1 AL 5)
	Robo		
	Vandalismo		
	Falla de Equipos (hard)		
	Virus		
	Equivocaciones		
	Accesos no Autorizados		
	Robos de Datos		
	Caída de Servicios en/los Servidores		
	Rotura de Enlace		
	Contaminación		
	Disparo de Protección Térmica		
	Fallo en caja de Conexión		
	Fallo en los Patch Cord		
	Error de Configuración		
	Error de Software		
	Fuego		
	Fraude		
	Terremoto		



Analizando este cuadro se obtienen los riesgos con impacto y probabilidad alta, los cuales deberán ser considerados para generar el Plan de Acción.

Para el resto de los riesgos se determinaran las recomendaciones y medidas necesarias que serán de menor grado que las consideradas en el Plan de Acción.

2) Realizar a criterio las acciones a tomar para los riesgos considerados en la tabla.

3.4 Filminas

Las filminas son el modelo a seguir en la concientización y capacitación del seminario, las cuales están sujetas a las modificaciones necesarias, que surjan en la preparación del mismo.

Los contenidos son extraídos de la actividad N°1, "Requisitos Mínimos para planes de contingencias" de este mismo contrato de Mitigación de riesgos.

Presentación Usuario.ppt

Presentación Gerente.ppt

Presentación Informatico.ppt

Seminario orientado a

Planes de Contingencias

Destinatario: Usuario Final

Secretaria de Estado de Tecnologia de la Información

Gerencia de Servicios San Luis – Gerencia de Concientización Comunitaria

Planes de Contingencias

Una **Contingencia** es un ataque o amenaza que pueda sufrir la organización o sector de trabajo de manera impredecible

Contingencia de Origen Mixto: (Naturales y Provocados por el Hombre):

- **Ambientales: Inundación – Fuego – Catástrofes climáticas**
- **Fallas de Corriente Eléctrica**
- **Contaminación**
- **Amenazas del lugar o Ubicación de la Organización u oficinas**
- **Fallas de Hardware y Software**
- **Robo**
- **Otras.**

Un **Plan de contingencia** es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. *Los planes de contingencia también se conocen como planes de continuidad*

Procedimientos y Actividades a realizar

- **Informarse y aplicar las políticas de seguridad de la Organización.**
- **Identificar a los responsables de Seguridad y Planes de Contingencias del área.**
- **Determinar planes de respaldo que incluyan procedimientos manuales para casos de interrupción en los servicios de procesamiento de datos (tales como los procedimientos de backups).**

Realizar las actividades a nivel usuario

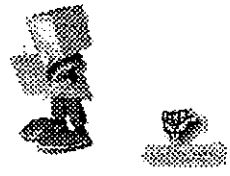
- **Mantenimiento de la limpieza de los equipos y del lugar de trabajo.**
- **Evitar comer, fumar y beber sobre los equipos.**
- **Actualización periódica del antivirus existente.**
- **Exigir que los equipos estén conectados a una UPS o fuente de Tensión**
- **Realizar periodicamente backups en algun medio magnético: Cds, diskettes, red, zip, etc.**

Existen tres tipos de Backups

Backups Completo: Incluye todos los archivos de un tipo, de una unidad, directorio, etc.

Backups Progresivo: Solo copiará aquellos archivos que hayan sufrido algun cambio desde la útima copia de Seguridad.

Backups Diferencial: copiará aquellos archivos que hayan sufrido algun cambio desde la última copia de seguridad completa realizada.

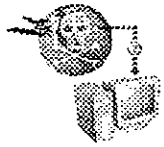


En cuanto a la prevención General debemos Considerar las 11 maximas siguientes:

1. Utilizá ANTIVIRUS y actualizalo siempre

2. Aseguráte de que esté siempre activo

3. Usalo siempre antes de abrir los mensajes de correo electrónico



4. No descargues programas de Internet de lugares que no sean seguros

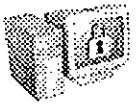
5. Analizá SIEMPRE los diskettes que vayas a utilizar en tu PC.

6. Sacá los diskettes de la PC cuando la arranques o la apagues

7. Analizá siempre el contenido de los archivos comprimidos (Zipeados)

8. Utilizá siempre las opciones de SEGURIDAD de los programas en tu PC

9. Todas las semanas, como mínimo, realizá copias de seguridad (Backup) de la información de tu PC



10. Mantenéte informado acerca de todas las novedades en estos temas.

11. Utilizá siempre SOFTWARE LEGAL

Es importante destacar la documentación.
Dada una contingencia se debe documentar de cierta forma lo sucedido,tratando de encontrar :

- **Causa o motivo que la provocó**
- **Grado de daños ocacionados**

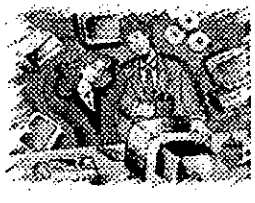
Para lograr

- **Identificar con anterioridad las situaciones que lo provocan.**
- **Desarrollar las actividades preventivas**

Conclusión

Se debe tener presente que administrar la calidad y el funcionamiento continuo es responsabilidad compartida por todos en una Organización para lograr que no existan defectos o imprevistos.

Mientras mas temprano se detecte y prevenga un problema más fácil será su control y eliminación.



Seminario orientado a:

Planes de Contingencias

Destinado al Nivel Gerencial

Secretaria de Estado de Tecnología de la Información

Gerencia de Servicios San Luis – Gerencia de Concientización Comunitaria

Introducción

La producción y el trabajo están asociadas a la Concientización (tomar acciones) y a la Capacitación.

Estos conceptos nos llevan a un proceso de adaptación y de cambio de pensamiento, los cuales mediante un factor importante que también interviene como la motivación, tal vez podamos comprender la necesidad y el beneficio que nos da la prevención ante cualquier eventualidad.

Cambio

"La forma de pensar actual no nos lleva a nada productivo"

- ✓ Confiarse de que esta todo controlado.
- ✓ Realizar copias de mi trabajo sin pensar si mi personal a cargo lo esta realizando al igual que yo.
- ✓ No contar con un plan de Contingencias para mi organización.

Motivación y Concientización

Para este caso estos conceptos deben surgir de la necesidad de conservar, la información de la organización o Área que la hace funcional.

Concientizarnos y concientizar de la importancia que tiene el adquirir o desarrollar un Plan de Seguridad y uno alternativo llamado **Plan de Contingencias**

¿Cuando Tomamos conciencia?

Todas las empresas están perfectamente preparadas para afrontar con éxito un desastre en el sistema de información... la segunda vez que lo sufren

Hoy en día, la mayor parte de los datos de una empresa están almacenados en los equipos informáticos. Cualquier problema en los sistemas de información repercute instantáneamente en la totalidad de la empresa y afecta al funcionamiento normal.

La prevención es requerida para:

- Proteger la inverción en Informética
- Que la Organización sobreviva a un desastre
- Mantenerse en evolución tecnológica (no volver en el tiempo
- La prevención, detección y protección de sucesos que afecten negativamente a la organización.

Los procedimientos...

- ✓ **Los procedimientos de Planes de Contingencias deben de emanar de la máxima autoridad Institucional para garantizar su difusión y estricto cumplimiento.**
- ✓ **Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento.**
- ✓ **En estos procedimientos estará involucrado todo el personal de la Organización.**

¿Como designamos los equipos operativos...?

Se debe designar un responsable por cada Área Operativa, el cual realizara entre otras las siguientes actividades:

- ➢ **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 y subsistemas**
- ➢ **Supervisar los procedimientos de respaldo y restauración**

- **Coordinar líneas, módems, terminales, etc. Para comunicaciones**
- **Establecer procedimientos de seguridad en los sitios de recuperación.**
- **Organizar pruebas de Hardware y software.**
- **Ejecutar trabajos de recuperación.**
- **Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante**
- **Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante**
- **Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación**

Conclusión:

Debe hacerse notar que conforme mas gente de la organización obtenga mayor poder de acceso, la seguridad llega a ser cada vez mas difícil y compleja.
La existencia de amenazas que afectan la disponibilidad, integridad y confiabilidad de los datos es Real.
Por ello es importante definir los procedimientos y Planes de Contingencias, para el caso de una posible falla, siniestro o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora.

Seminario orientado a

Planes de Contingencias

Destinatario: Nivel Informático

Secretaria de Estado de Tecnología de la Información

Gerencia de Servicios San Luis – Gerencia de Concientización Comunitaria

Autopista de la Información

PRESENTACIÓN

Ante la presencia ineludible de riesgos en cualquier actividad laboral, es indispensable saber cómo debe actuar cada organización según la gravedad de los casos.
No basta con buenas intenciones.
Es necesario prepararse, tomar conciencia, organizarse. Si ello no ocurre, la alternativa no es otra que asumir el riesgo.
Para ello se diseñan los
PLANES DE CONTINGENCIA.

Plan de Contingencias

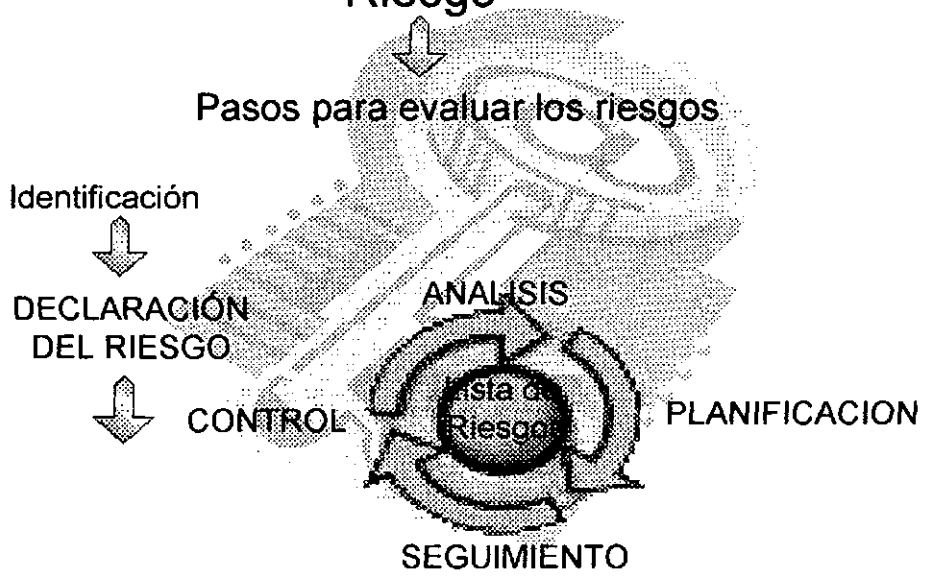
Un plan alternativo que se desarrolla para paliar cualquier ataque que penetre los sistemas, el equipamiento o la red.

Planificar detalladamente las reacciones ante cada tipo de contingencia

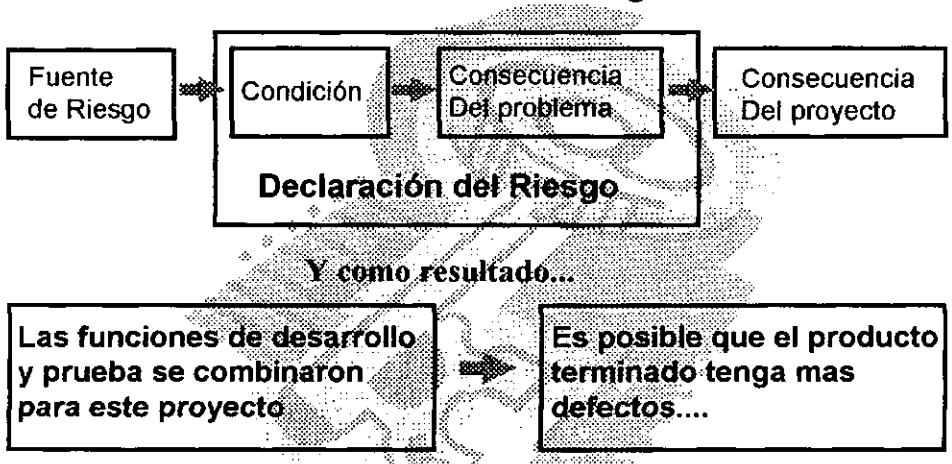
El Riesgo

Riesgo

Pasos para evaluar los riesgos



Valoración del Riesgo



Y como resultado...

Las funciones de desarrollo y prueba se combinaron para este proyecto ➡ **Es posible que el producto terminado tenga mas defectos....**

Un riesgo debe declararse con claridad ante de poder Administrarlo.

Una vez identificados los riesgos se definen las actividades para desarrollar un plan de contingencias.

✓**Determinar quién debe hacer qué, en qué momento y en qué lugar para que la organización siga funcionando.**

✓**Abarcar la restauración de las copias de seguridad.**

✓**Ensayarse periódicamente para mantener al personal informado de los pasos de la contingencia actual.**

✓**Explicar la actualización del software antivirus.**

✓**Abarcar el traspaso de la producción a otra ubicación o sitio.**

Las actividades a contemplar se dividen en 3 (tres) etapas.

Antes | Durante | Despúes

De la Contingencia

Antes de la Contingencia

Establecimiento del Plan de Acción.

- ✓Sistemas Informáticos
- ✓Equipos Informaticos
- ✓Politicas y Procedimientos de Backups

Formación de Equipos Operativos.
Se deberá designar un Referente informático para la seguridad de la Información de su unidad. Pudiendo ser el encargado de dicha Área Operativa.

Formación de Equipos de Evaluación (auditoria de cumplimiento de los procedimientos de Prevención y Seguridad).
Esta función debe ser realizada de preferencia por personal externo.

Durante la Contingencia

Plan de Emergencias

En este plan se establecen las acciones que se deben realiza cuando se presente una contingencia, así como la difusión d las mismas

Formación de Equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante una Contingencia.

Entrenamiento

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

Después de la Contingencia

Evaluación de los daños

Control de recuperación y Restauración

Documentar y aprender

Actualización de directivas y controles de seguridad

CONCLUSIÓN

Se ha podido observar que para hacer una planeación eficaz de contingencias sobre una organización, lo primero que se requiere es información general sobre la misma y sobre la función del Area de sistemas a evaluar. Para ello es preciso hacer una investigación preliminar mediante entrevistas, encuestas, etc.y con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costos, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

4. CONCLUSIÓN

Para lograr que un seminario tenga éxito en la comunicación, es necesario estar siempre alertas, siempre conscientes de lo que decimos.

Es importante tener en claro que la formación de hábitos y de actitudes forma parte de la tarea cuando queremos trasmitir algo. Estos hábitos no se limitan a lo que el hombre hace. Comprenden también las actitudes. Formar hábitos es una manera constructiva de enfrentarse a los hechos de la vida, por los cuales se van descubriendo medios para alcanzar un fin deseado o para resolver un problema satisfactoriamente. Y una vez encontrado ese medio, el hombre trata de convertir sus actitudes y acciones en un procedimiento uniforme.

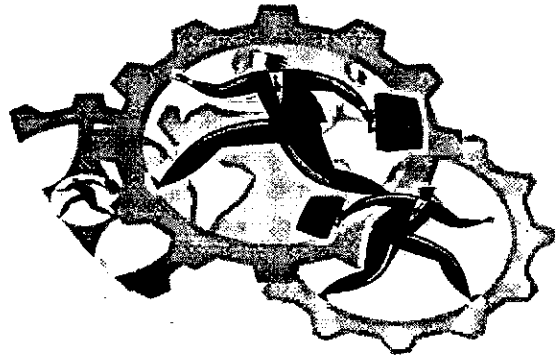
Los hábitos incluyen tanto actitudes como acciones. Como la actitud es una inclinación permanente a reaccionar de cierta manera cada vez que respondemos a una situación determinada. Es muy importante, que debido a esto, adquiramos actitudes positivas si queremos desarrollar una comunicación amena, para lograr nuestro objetivo de concientizar y capacitar a nuestro personal.

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

ELABORACIÓN DE PLANES DE CONTINGENCIA



ANEXO I

Actividad N°1

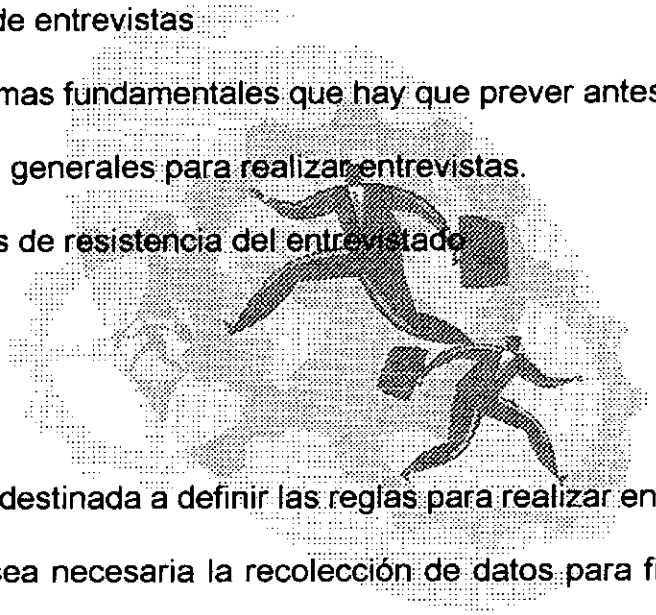
"TÉCNICA DE LA ENTREVISTA"

ANEXO I

TÉCNICA DE ENTREVISTA

Esta técnica fue incorporada de la Actividad N°9 Proyecto de Redes **"Relevamiento Integral Del Funcionamiento Del Estado Provincial En El Manejo De La Información"** la cual posee los siguiente tópicos a tener en cuenta:

1. Enunciado
2. Cuerpo
    2.1. Tipos de entrevistas
    2.2. Problemas fundamentales que hay que prever antes y durante la entrevista.
    2.3. Reglas generales para realizar entrevistas.
    2.4. Formas de resistencia del entrevistado
3. Conclusión



1. Enunciado

Esta técnica esta destinada a definir las reglas para realizar entrevistas, para cualquier situación donde sea necesaria la recolección de datos para fines definidos, pudiendo planificarse en forma ordenada la obtención de la información necesaria.

Cuerpo

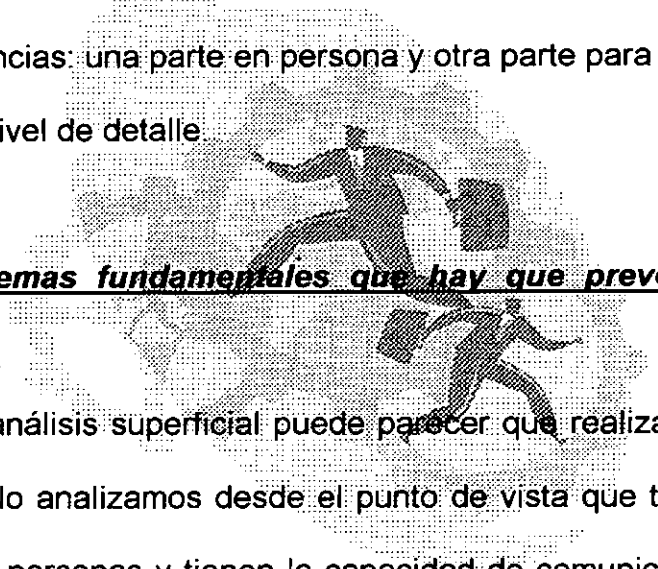
2.1. Tipos de entrevistas

La forma de entrevista habitual es el encuentro persona- persona, en todas sus alternativas: un grupo de entrevistadores con un entrevistado, un entrevistador con un grupo de entrevistados, dos grupos. Normalmente uno o mas de los entrevistadores toma nota en papel, también tiende a usarse un grabador, aunque es menos común. (a partir de aquí podremos llamar al entrevistador analista y al entrevistado usuario)

Como punto de partida para este trabajo asumiremos que la entrevista se realiza dentro de los parámetros mas generales que se encuadran en tomar notas en papel.

Debe tenerse en cuenta que hay información que se puede obtener fuera de la entrevista, a través de otros medios, solicitando al entrevistado que complete una encuesta formal preparada con anterioridad, o solicitando información ya existente en el área. Puede existir información de la requerida que ya haya sido relevada con anterioridad.

Una alternativa no es excluyente de la otra, puede preverse una entrevista que cuente con ambas presencias: una parte en persona y otra parte para responder por escrito, si se requiere otro nivel de detalle.



2.2. Problemas fundamentales que hay que prever antes y durante la entrevista.

Si se realiza un análisis superficial puede parecer que realizar una entrevista es una tarea sencilla, si lo analizamos desde el punto de vista que tanto entrevistado, como entrevistador son personas y tienen la capacidad de comunicarse, con racionalidad y capacidades y ambos son capaces de lograr el mismo objetivo: transferir información.

Entonces ¿Cuál es el problema?

Existen muchos problemas porque por el mismo hecho de ser personas hay una motivación intrínseca de cada uno que puede derivar en una entrevista poco eficiente.

Los problemas más comunes que podemos tener en cuenta son los siguientes:

✓ Entrevistar a las personas equivocadas en el momento equivocado: es muy factible, dados los problemas de cada organización, que se encuentre hablando con la persona que "oficialmente" es el conocedor a fondeo del tema pero que resulta no saber nada de los verdaderos movimientos de información dentro del área que le compete, y así es

posible perder de vista a aquella persona que si conoce lo que nosotros necesitamos saber.

Aun si estamos con la persona correcta, pude darse que se le esta realizando una entrevista en un momento que no esta disponible, sometido a determinadas presiones externas y debe acceder a la entrevista porque ha sido ordenado desde un nivel mas alto.

✓ Hacer las preguntas equivocadas: normalmente el entrevistador (analista) y el entrevistado (usuario) tienen distinto vocabulario, distinta experiencia, y, a menudo, distintas percepciones, valores y prioridades. Por esto es factible que se realice una pregunta razonable al entrevistado, que este la malentienda y ninguno de los dos se percate de ello.

Es factible también que el usuario de información y que el entrevistador no comprenda bien esa información, nuevamente sin que ninguno de los dos se percate.

Por esto es importante plantear un lenguaje claro, entendible para las dos partes y revisar todas las preguntas y respuestas para asegurarse de que haya un verdadero entendimiento de cada una de ellas.

✓ Crear fricciones: puede ser que el usuario se sienta incomodo o presionado, probablemente por el consabido temor a que lo que sabe es lo que lo mantiene en su puesto y si transmite esta información puede perder su empleo.

Por otra parte el analista puede sentirse molesto e irritado por la forma en que el usuario esta respondiendo, o por constantes interrupciones o porque el usuario sustenta un alto cargo jerárquico y hace notar la diferencia con el entrevistador.

En cualquiera de los casos pueden surgir fricciones y crear situaciones incomodas que lleguen a una entrevista fallida.

No hay manera de asegurarse que estos problemas no surjan, ni de garantizar el éxito de la entrevista, porque, reiteramos, se trata de interacción entre personas y cada una de las relaciones que se establece es única sin embargo se pueden cumplir una serie de reglas que pueden llegar a lograr que la entrevista sea exitosa, previendo los problemas y haciendo todo los posible para evitarlos.

2.3. Reglas para realizar entrevistas

a) Desarrollar un plan global de la entrevista: Antes que nada es importante saber a quien se entrevistará, esto requiere obtener un organigrama que muestre los distintos puestos y funciones. Si no existe uno hay que armarlo y si el que existe esta desactualizado hay que solicitar la ayuda de quien este capacitado para ayudarnos a actualizarlo. También es necesario durante todo el proceso de realización de entrevistas realizar un cronograma y mantener ambos (organigrama y cronograma) actualizados.

   Es importante determinar cuales son las funciones y el cargo que desempeña el entrevistado y, en caso de ser posible, conseguir toda otra información referente al mismo de quienes los puede conocer, de manera tal que el analista vaya preparado para saber que tipo de persona es su usuario, que tipo de conocimientos posee y cuales son las características del puesto que desempeña.

   También es importante hablar con ellos en la secuencia apropiada y la combinación correcta. Si hay áreas interrelacionadas hay que analizar previamente la situación para poder saber a quien y en que orden se debe entrevistar, y si conviene en alguna ocasión entrevistar a mas de una persona en el mismo momento.

b) Contar con la aprobación necesaria para poder realizar las entrevistas a los usuarios: Es poco común una organización tan informal (carente de organización interna jerárquica) donde se pueda ir por ahí realizando entrevistas, en general es

políticamente peligroso y poco recomendado hacerlo sin contar con la autorización de los niveles jerárquicos a quienes compete la misma.

En todo caso la autoridad competente tiene legítimos motivos para querer saber con anticipación a quienes y cómo se los va a entrevistar:

✓ Puede suceder que algunos usuarios no sean capaces de entender o describir bien los datos necesarios o correctos.

✓ Puede suceder que algunos usuarios, por temor, den datos que no son verdaderos.

✓ Puede generar situaciones donde se interfiera con la labores normales de los entrevistados y querrán programarlas.

✓ Pueden las entrevistas generar una sensación de que el trabajo humano será reemplazado por sistemas computarizados, generando una sensación de desasosiego poco deseable en el funcionamiento habitual del a organización.

✓ Puede suceder que ellos sepan mas que los operativos de los requerimientos de la encuesta.

✓ Puede existir algún conflicto político a un nivel mas alto que el de la administración.

Estas son algunas de las razones por las cuales es aconsejable conseguir una autorización antes de realizar las entrevistas

c) Planear la entrevista para que sea efectiva en el tiempo usado para la misma: es necesario "robarle " el menor tiempo posible al usuario, dado que este puede pensar que es "una perdida de tiempo" la misma. Por eso es necesario planearla con anticipación para hacerla más eficiente y productiva tanto para le entrevistador como para el entrevistado.

Si antes de realizarla se plantea un tiempo determinado es absolutamente necesario respetar el mismo, excepto en caso de factores externos que la demoren

(llamadas telefónicas, reuniones imprevistas, mayor cúmulo de información prevista o analizada).

Lo primero que hay que hacer es informar al entrevistado del tema de la misma, puede ser vía teléfono al solicitar la misma, por correo electrónico o enviándoles con dos días de anticipación la encuesta. Si el usuario llega a la entrevista sin saber de que se trata puede deberse a diferentes motivos (esta muy ocupado, no le interesa, siente hostilidad a los cambios, no es capaz de entender el concepto, etc.).

Además se debe reunir todo tipo de información antes de la entrevista, sobre todo si se han realizado algunos relevamientos previos, a fin de no plantear una y otra vez los mismos temas y que el usuario diga " esto ya me lo preguntaron cien veces" Asegúrese de obtener esta información y estudiarla antes de la entrevista.

Se recomienda no planificar una entrevista que supere las dos horas, no solo por el abuso del tiempo del entrevistado, que estará postergando otras actividades para atenderlo, sino porque el nivel de concentración de las personas empieza a decaer luego de ese tiempo, en caso de requerir mas tiempo se recomienda realizar un break o dejarlo para días posteriores, aunque no muy alejados del primer encuentro para que no se escape el interés por el tema.

Finalmente programe una reunión de seguimiento del material consolidado, una vez pasado a formato digital, hágaselo llegar al entrevistado para que el lo revise y le de el visto bueno o realice las correcciones necesarias. Tenga en cuenta que probablemente los datos se analizarán, manipularán, documentarán y se transformarán a una forma que posiblemente el usuario jamás haya visto antes y por eso es importante asegurarse de que no haya entendido mal lo que el usuario le dijo, que este no haya cambiado de opinión desde la entrevista y que el entienda la representación gráfica de dichos resultados.

d) Interesar al usuario en el tema de la entrevista: es importante que el entrevistado se comprometa e involucre personalmente con el tema de la entrevista, que lo sienta como propio, que se sienta participe de un proyecto, como un eslabón útil para que ofrezca su colaboración total y francamente. Lo mas lógico es mostrarle cual será el beneficio, a corto o largo, plazo que obtendrá, de los datos emanados de la entrevista.

e) Utilizar un estilo apropiado de entrevista: realizar preguntas de sondeo no es sencillo, depende de la personalidad del entrevistado y del interés que despierte en él el tema de la entrevista, puede ser que se requiera una variedad de estilos para lograr la información deseada:

- Relaciones: Solicite al usuario que establezca relaciones entre lo que esta expresando y otra información recabada del área. Incluso las relaciones con otros datos que ya se hayan recabado en otra área, por ejemplo si una repartición le informo que pasa una x cantidad de datos al área del actual entrevistado, confirme con él que esto sea verídico y que se da en las mismas condiciones citadas por el otro entrevistado.

  Esto no solo ayuda a obtener mayor y mejor información sino que también lo ayudará a descubrir interfaces, flujos de datos y relaciones formales.

- Puntos de vista alternativos: Solicite al usuario que describa puntos de vista de otros usuarios, tanto sean de nivel jerárquico superior o inferior. Es importante abrir el espectro de posibilidades todo lo que se pueda.

- Sondeo: Solicite al entrevistado que le cuente "informalmente" de aquella información que le interesa obtener, por ejemplo "Cuénteme acerca de cómo realizan internamente los tramites de expedientes"

- Dependencias: Solicite al usuario que le diga si hay otros factores que incidan sobre el manejo de la información que esta recolectando. Por ejemplo si esa información para ser procesada requiere cumplir algún paso previo que debe ejecutar otra área o dependencia.
- Repetición: Repítale al usuarios lo que cree que le quiso decir pero con sus propias palabra para que lo confirme, puede decir: " A ver si entendí...."

2.4. Formas de Resistencia a ser entrevistado

Este es un punto crucial para tener en cuenta y para estar preparados cuando se enfrente la situación de una fuerte resistencia por parte del entrevistado.

Algunas razones de las mas comunes del entrevistado para evitar la encuesta son:

- "Están ocupando demasiado del poco tiempo que tengo": Una buena alternativa para paliar esta respuesta es decirle " Estoy convencido de que tiene razón y le pido disculpas por ello pero quisiera que me permita decirle que he preparado la entrevista y esto reducirá al mínimo el tiempo que le demandará, además me he preparado y tengo algunos conocimientos previos para no sacarle tanto tiempo". Se requiere ser puntual y no salirse nunca del objetivo planteado y que cumpla fielmente con lo prometido.

  Esto también tendrá como ventaja adicional que Ud. obtendrá un viso de respeto por parte del entrevistado por su cumplimiento de las normas preestablecidas entre ambos.

- "Es una forma de probar que no estoy capacitado y de sacarme mi lugar de trabajo" Esta idea puede no expresarse directamente y venir oculta detrás de un manto de excusas pero siempre esta el mensaje subliminal del temor a perder el lugar de trabajo, el puesto, por lo desconocido que se avecina.

Pero se debe tener en cuenta que esta es una reacción mas emocional que racional y puede o no tener asideros reales. Aunque hay una gran variedad de respuestas debe recordar que el entrevistador no es el responsable de asegurarle al usuario que su puesto de trabajo es seguro y le daría una falta de credibilidad asegurar tal cosa. Se puede deslindar responsabilidad diciendo: " No soy yo quien puede asegurarle o no que esta en lo cierto, pero yo solo estoy recolectando información que será beneficiosa para el área en la cual Ud. se desempeña y para la organización en general" Es poco probable que el usuario acepte una respuesta de este tipo y lo asumirá como que se " esta lavando las manos" o incluso que sabe mas de lo que quiere decir y que en realidad esta aconsejando a los altos niveles de decisión de la organización como reemplazar su empleo mediante una PC.

La solución mas viable sería, en caso de presentarse este inconveniente, informárselo al responsable que le ha autorizado a realizar la entrevista, de esta resistencia del usuario y que sean ellos quienes tomen la responsabilidad en sus manos de encontrar la solución y asumir la responsabilidad de las consecuencias.

- "No sabe nada de esta repartición ¿Cómo puede estar capacitado para recibir y procesar la información que le doy?" Sería aconsejable responder a esto diciendo "Ud. tiene razón. Es por ello que estoy recurriendo a Ud. que tiene mas experiencia para conocer su opinión" También puede sugerir maneras de "mejorar" las cosas, sobre todo si parte del trabajo que realiza el usuario esta sujeto a viejas reglamentaciones que solo lo llevan a usar mas tiempo y ser menos eficaz o incluso a cometer errores.

Lo mas adecuado es continuar siendo muy humilde y reconocer constantemente la experticia del entrevistado en su área de trabajo, pero siempre teniendo en cuenta

que si su posición es falsa el entrevistado puede sentirla y volverse un punto en su contra.

- "Trata de cambiar la forma en que hacemos las cosas, cuando todo aquí funciona perfectamente". En este caso debe hacerle entender que aunque algunos cambios, aunque sean radicales, en la implementación de un sistema, no cambiará las características esenciales, solo que ayudará a mejorar la eficacia y productividad de los usuarios del mismo.
- "No me interesa informatizar nada, estamos bien como estamos" Esta es una variante de "me quiere sacar el empleo" y esta marcada por el temor que todavía genera el uso de una PC, sobre todo en los usuarios de mayor edad. La realidad es que "el que manda" quiere implementar un sistema y no esta en las funciones del entrevistador convencer al usuario de que esto debe ser así. La verdadera respuesta es que el entrevistador está allí, realizando la misma y que eso es inmodificable porque la decisión no corresponde ni al usuario ni al analista.

4- Conclusión

Las habilidades de comunicación, la diplomacia y demás cuestiones humanas involucradas en el desarrollo de una entrevista NO son cuestiones sencillas que se pueden abarcar en una técnica. Por lo tanto en la presente se han dejado establecidas las pautas generales para comenzar a usar la técnica.

Estas características mencionadas deben ser aprendidas con el tiempo, con las características intrínsecas de cada entrevistador y con practica y observación. Es recomendable que un entrevistador novato realice algunas entrevistas con uno veterano que podrá transmitirle algunas reglas tácitas en lo que se refiere al trato con otras personas. Pero siempre hay que tener presente que para poder llegar al punto de unión se debe estar atento a las necesidades del usuario, escucharlo y aprender de sus

requerimientos para lograr por ese camino (aunque este a veces represente un "camino paralelo") obtener la información que realmente se necesita.

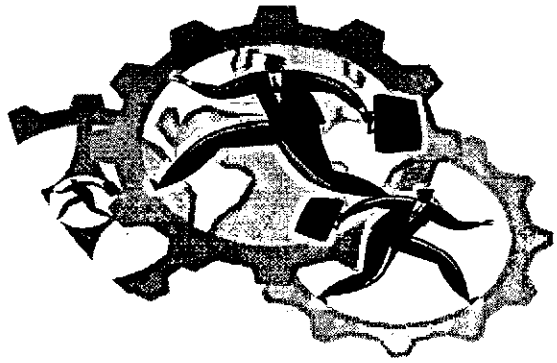
Es importante tener en cuenta la retroalimentación desde dos variantes: el superior del entrevistador puede hablar con los entrevistados para conocer su opinión acerca de cómo realizarlas entrevistas y en segundo lugar hacia los usuarios informándoles como se usarán los resultados de las entrevistas, para que quede instalada la idea de que todo fue en vano.

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

ELABORACIÓN DE PLANES DE CONTINGENCIA



ANEXO II

Actividad N°1

"MODELOS DE CUESTIONARIOS"

ANEXO II

MODELOS DE CUESTIONARIOS

Modelo Nota Presentación y aval

San Luis, 7 de Mayo de 2001

Sres :

Telefónica Argentina S.A.

S_____/_____D

Me dirijo a Uds. a fin de solicitar vuestra autorización para que profesionales que se encuentran trabajando para el Gobierno de la Provincia de San Luis puedan realizar un relevamiento y entrevistas en esa Organización, con el objeto de obtener datos sobre Planes de Contingencias y Seguridad, vigentes en ámbitos informáticos y que no violen la privacidad de la organización.

Los mismos se usarán para realizar un estudio y análisis de las opciones mas optimas y eficaces, que existen en el mercado actual en organizaciones de gran envergadura, para poder elaborar de esta manera los Planes de Contingencias y Seguridad, aplicables a la Intranet de la Provincia de San Luis, en un todo de acuerdo con los métodos actuales vigentes en el mercado.

Esta información será solicitada a varias organizaciones provinciales y de nivel nacional e internacional por profesionales que trabajan para el Consejo Federal de Inversiones (CFI) en el Proyecto Mitigación de Riesgos, el mismo se desarrolla actualmente para la Gerencia de Servicios San Luis dependiente de

la Secretaria de Estado de Tecnologías y de Información del Gobierno de la Provincia de San Luis.

A los fines que hubiere lugar, se adjunta modelo de cuestionario que contiene la información a requerir.

Agradeciendo desde ya su colaboración, saludoles atentamente.

Arq. Ana Sáenz de Gatica

Secretaria de Estado de Tecnologías de la Información

Cuestionario A

(*En Caso de Contar con Material para entregar, verificar si es necesario continuar con el cuestionario*)

1 ¿ Poseen un listado de los riesgos o eventualidades consideradas?

2 ¿ Cual es la evaluación económica de estos sucesos negativos?

3 ¿Cual es el Análisis efectuado de las consecuencias de dichos riesgos?

4 ¿Cuál es la fiabilidad de los datos obtenidos?

5 ¿Qué es lo que se intenta proteger?

6 ¿Cuál es su valor para cada uno o para la organización?

7 ¿Cuál es la probabilidad de un ataque?

8 ¿A que riesgos en la seguridad informática se enfrenta la institución?

9 ¿La Organización esta certificada por las normas ISO?

10 ¿La Organización esta inscripta o cubierta por una ART?

11 ¿Qué probabilidad hay de que tenga efecto alguno los riesgos mencionados?

Por ejemplo en:

Fuego

¿La institución cuenta con protección contra incendios?

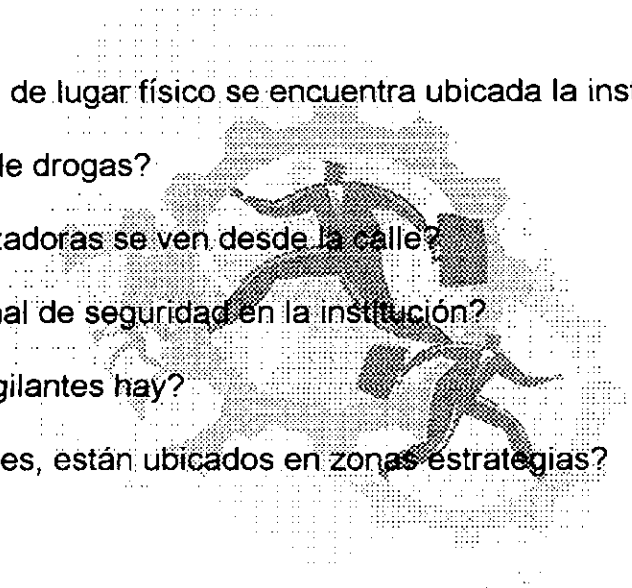
¿Se cuenta con sistema de aspersión automática?

¿Diversos extintores?

¿Detectores de humo?

¿Los empleados están preparados para enfrentar un posible incendio?

Robo



¿En que tipo de lugar físico se encuentra ubicada la institución u empresa?

¿hay venta de drogas?

¿Las computadoras se ven desde la calle?

¿Hay personal de seguridad en la institución?

¿Cuántos vigilantes hay?

¿Los vigilantes, están ubicados en zonas estratégias?

Vandalismos

¿Existe la posibilidad que un ladrón desilusionado o frustrado cause daños?

¿Existe la probabilidad que causen algún otro tipo de daño intencionado?

Fallas de los Equipos

¿Los equipos tienen un mantenimiento continuo por parte del personal calificado?

¿Cuáles son las condiciones actuales de hardware?

¿Es posible predecir las fallas a que están expuestos los equipos?

Equivocaciones que perjudiquen

¿Cuántos saben los empleados de computadores y redes?

Los que no conocen del manejo de la computadora, ¿saben a quien pedir ayuda?

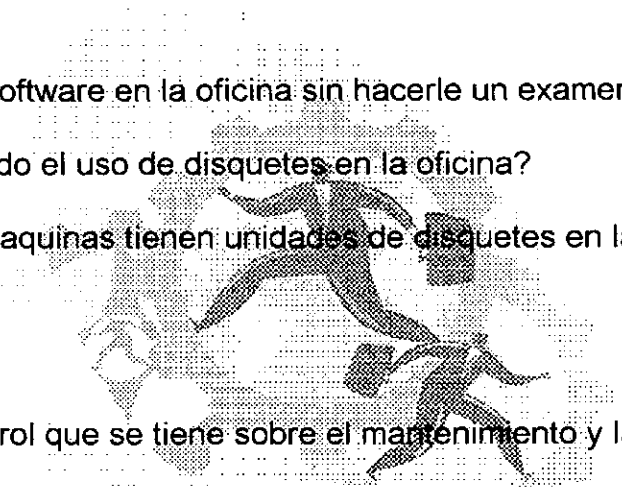
Durante el tiempo de vacaciones de los empleados ¿Qué tipo de personal los sustituyen que tanto saben del manejo de computadoras?

Virus

¿Se prueba software en la oficina sin hacerle un examen previo?

¿Está permitido el uso de disquetes en la oficina?

¿Todas las maquinas tienen unidades de disquetes en la oficina?



Cuestionario B

Para evaluar el control que se tiene sobre el mantenimiento y las fallas.

El objetivo de este cuestionario es evaluar la forma como se administran los dispositivos de almacenamiento básico de la dirección.

1. Los locales asignados a la cintoteca y discoteca tienen:

- Aire acondicionado ( )
- Protección contra el fuego ( )
- señalar que tipo de protección)_____
- Cerradura especial ( )
- Otra

2. ¿Tienen la cintoteca y discoteca protección automática contra el fuego?

SI ( ) NO ( )

(señalar de que tipo)_____

3. ¿Que información mínima contiene el inventario de la cintoteca y la discoteca?

Número de serie o carrete ( )

Número o clave del usuario ( )

Número del archivo lógico ( )

Nombre del sistema que lo genera ( )

Fecha de expiración del archivo ( )

Fecha de expiración del archivo ( )

Número de volumen ( )

Otros

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?

SI ( ) NO ( )

5. En caso de existir discrepancia entre las cintas o discos y su contenido, se resuelven y explican satisfactoriamente las discrepancias?

SI ( ) NO ( )

6. ¿Que tan frecuentes son estas discrepancias?

_____

7. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta a disco, el cual fue inadvertidamente destruido?

SI ( ) NO ( )

8. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?

SI ( ) NO ( )

¿Cómo?_____

9. ¿Existe un control estricto de las copias de estos archivos?

SI ( ) NO ( )

10. ¿Que medio se utiliza para almacenarlos?

Mueble con cerradura ( )

Bóveda ( )

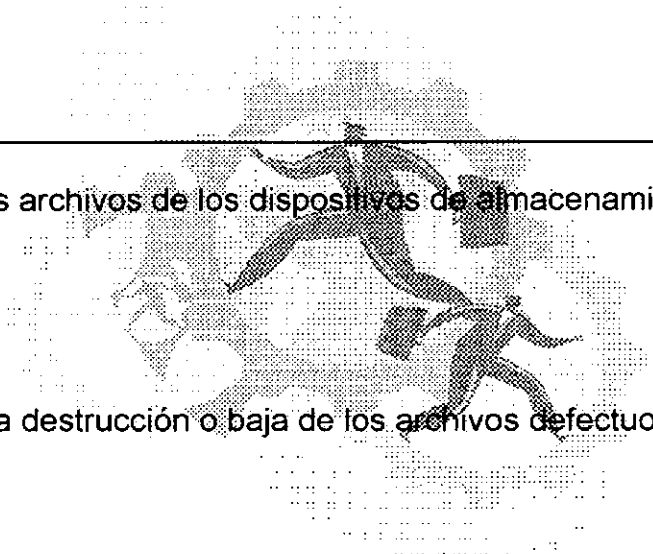
Otro(especifique)_____

11. Este almacén esta situado:

En el mismo edificio del departamento ( )

En otro lugar ( )

¿Cual?_____



12. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?

SI ( ) NO ( )

13. ¿Se certifica la destrucción o baja de los archivos defectuosos?

SI ( ) NO ( )

14. ¿Se registran como parte del inventario las nuevas cintas que recibe la biblioteca?

SI ( ) NO ( )

15 ¿Se tiene un responsable, por turno, de la cintoteca y discoteca?

SI ( ) NO ( )

16. ¿Se realizan auditorias periódicas a los medios de almacenamiento?

SI ( ) NO ( )

17. ¿Que medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

18. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?

SI ( ) NO ( )

19. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?

SI ( ) NO ( )

20. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?

SI ( ) NO ( )

21. ¿Se lleva control sobre los archivos prestados por la instalación?

SI ( ) NO ( )

22. En caso de préstamo ¿Conque información se documentan?

Nombre de la institución a quién se hace el préstamo.

- fecha de recepción ( )
- fecha en que se debe devolver ( )
- archivos que contiene ( )
- formatos ( )
- cifras de control ( )
- código de grabación ( )
- nombre del responsable que los presto ( )
- otros

23. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros:

24. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?

SI ( ) NO ( )

25. ¿El encargado de cintas, controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura?

SI ( ) NO ( )

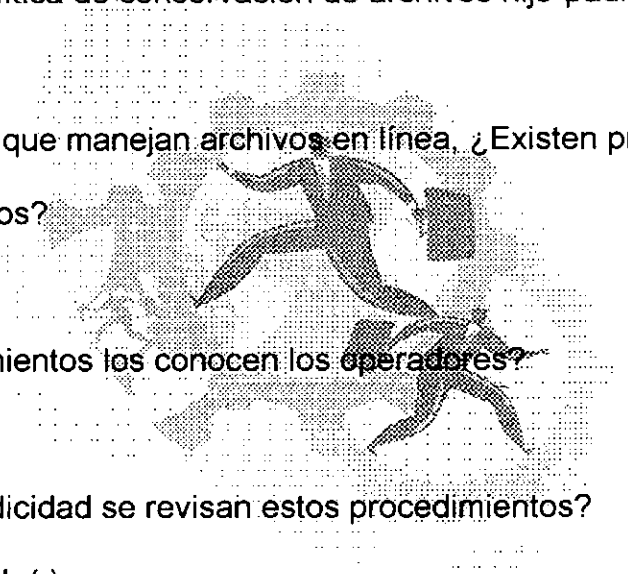
26. ¿La operación de reemplazo es controlada por el encargado de cintas?

SI ( ) NO ( )

27. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?

SI ( ) NO ( )

28. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?



SI ( ) NO ( )

29. ¿Estos procedimientos los conocen los operadores?

SI ( ) NO ( )

30. ¿Con que periodicidad se revisan estos procedimientos?

MENSUAL ( ) ANUAL ( )

SEMESTRAL ( ) OTRA ( )

31. ¿Existe un responsable en caso de falla?

SI ( ) NO ( )

32. ¿Explique que políticas se siguen para la obtención de archivos de respaldo?

33. ¿Existe un procedimiento para el manejo de la información de la cintoteca?

SI ( ) NO ( )

34. ¿Lo conoce y lo sigue el encargado de las cintas?

SI ( ) NO ( )

35. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programación informes de archivos para que liberen los dispositivos de almacenamiento?

SI ( ) NO ( )

¿Con qué frecuencia?

Cuestionario C (Realizado en las APP)

Ministerio:

Repartición o Area Dependiente;

Tel:

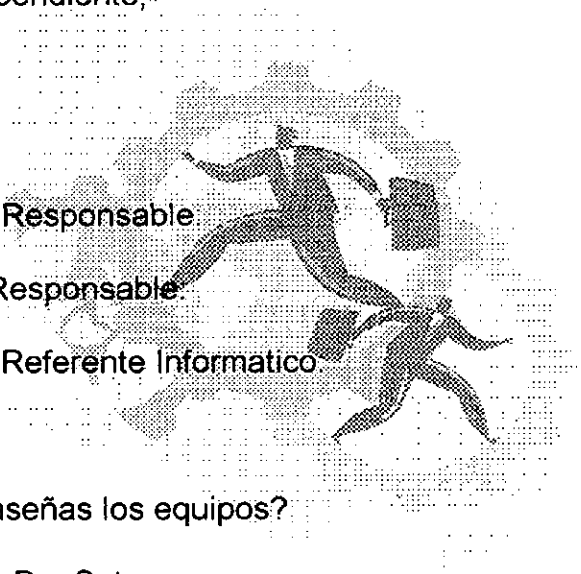
Ubicación Física:

Apellido y Nombre del Responsable:

Cargo o Función de l Responsable:

Nombre y Apellido del Referente Informatico:

Equipos:



1) ¿Utilizan Contraseñas los equipos?

   SI ( ) __ Por Setup

   __ Por Sistema Operativo

   NO ( )

2) ¿Trabajan en Red?

   SI ( ) __ con Intranet de Gobierno

   __ con Internet

   __ con servicio de Correo Electrónico

   NO ( )

3) ¿Se realizan Backups?

SI ( ) ¿Cada cuanto Tiempo? Diario__ Semanal__ Mensual__ Otros

¿Las Copias son a nivel: Usuario__ Intranet__ Subred___?

NO ( )

4) ¿Los equipos utilizan fuentes o UPS? SI ( ) NO ( )

5) ¿Se realizan mantenimiento de los equipos?

SI ( ) El mantenimiento es: Interno____ Externo____

NO ( )

6) ¿Hay directivas de procedimientos de trabajo que deben cumplir los usuarios?

SI ( ) NO( )

6) ¿Poseen antivirus instalados, actualizados?

SI ( ) ¿Cada cuanto tiempo? ___Diario

___Semanal

___Mensual

NO ( )

7) ¿Cual es el Software Utilizado?

Nombre (Aplicativo, Sistema Op. Etc.)

Fabricante:

Versión:

Licencias:

8) Software que necesita pero que no tiene:

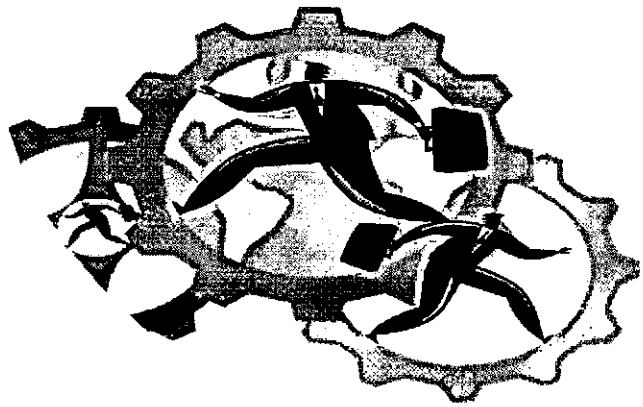
9) ¿Tienen previstos Planes de Contingencias? SI ( ) NO ( )

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

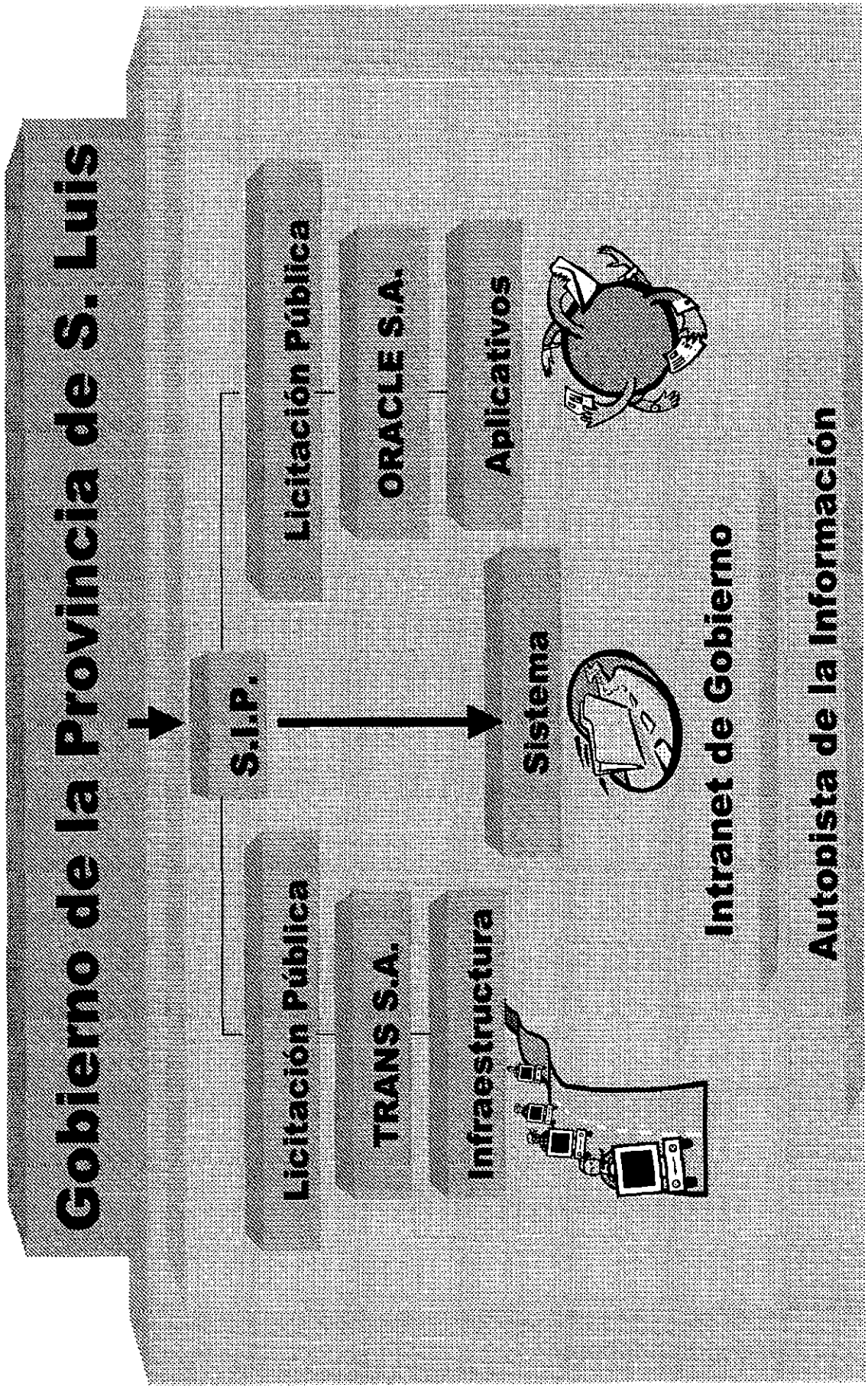
ELABORACIÓN DE PLANES DE CONTINGENCIA

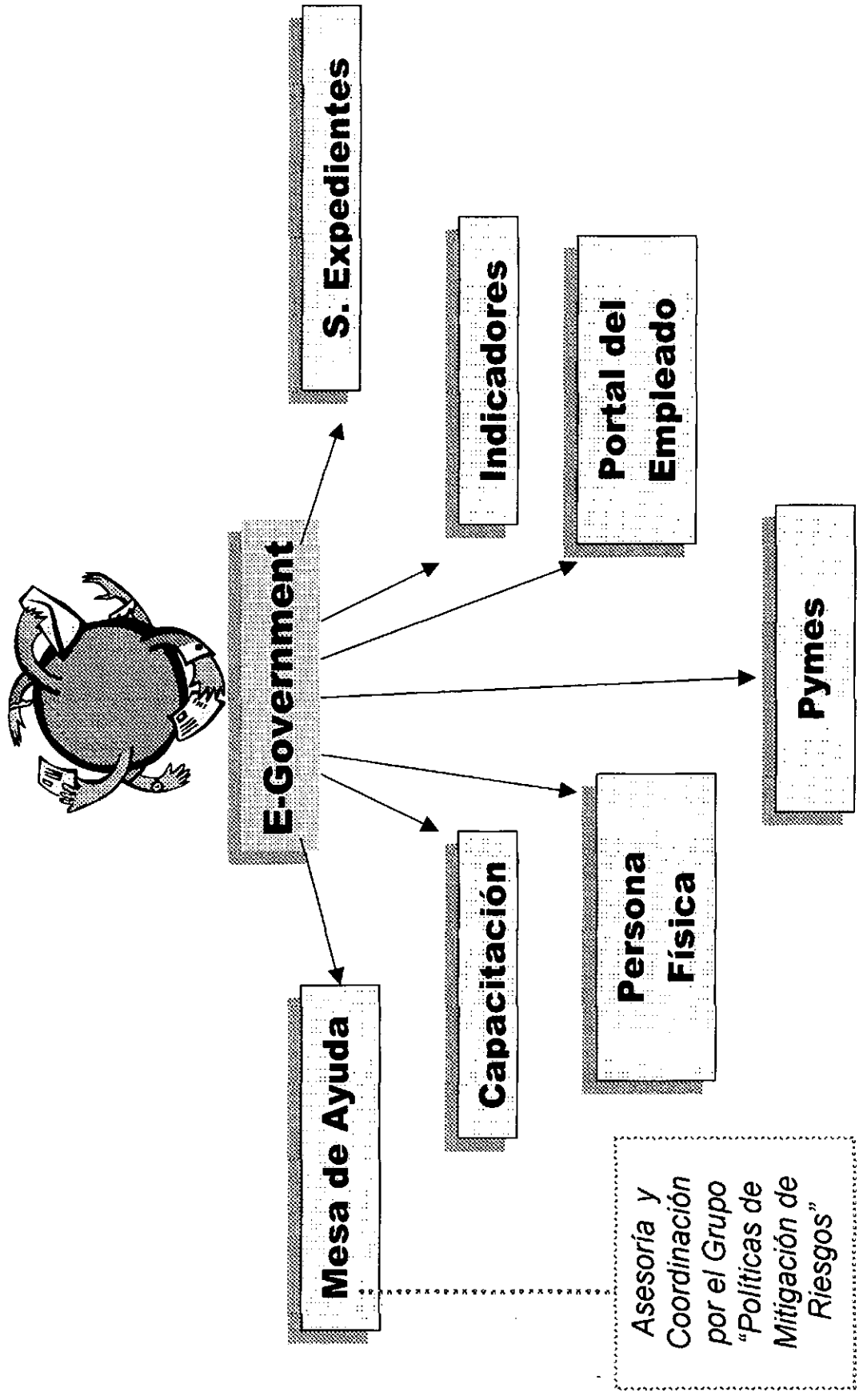


ANEXO III

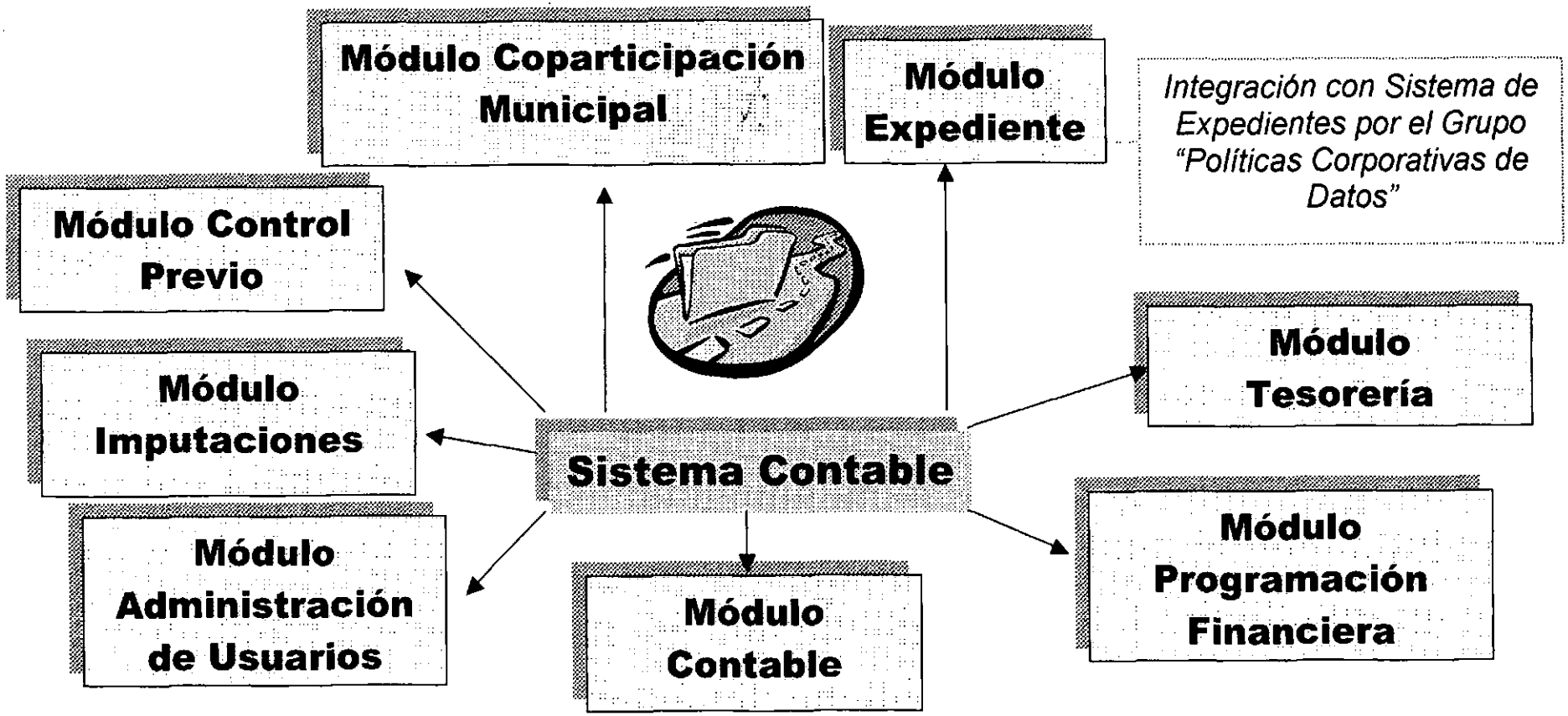
Actividad N°2

"CUADROS GRAFICOS DE LA ORGANIZACIÓN"


Gobierno de la Provincia de S. Luis
S.I.P.
Licitación Pública
ORACLE S.A.
Aplicativos
Licitación Pública
TRANS S.A.
Infraestructura
Sistema
Intranet de Gobierno
Autopista de la Información


S. Expedientes
Indicadores
Portal del Empleado
E-Government
Pymes
Capacitación
Persona Física
Mesa de Ayuda
Asesoría y Coordinación por el Grupo "Políticas de Mitigación de Riesgos"

Residencia del Gobernador
Hospital Regional
Hospital Materno
Edificio
Edificio Social Educativo
Edificio Junín e Illia
Casa de Gobierno Edificio
Red Física de la Intranet
Coordinación del Grupo "Redes Integradas"
Jefatura de Policía
Edificio PEHI
Centro Cívico V.M.
Edificio Canal 13
Edificio CREACyT
Casa de Gobierno Edificio Histórico
Edificio Arquitectura


Módulo Coparticipación Municipal
Módulo Expediente
Integración con Sistema de Expedientes por el Grupo "Políticas Corporativas de Datos"
Módulo Control Previo
Módulo Imputaciones
Módulo Tesorería
Sistema Contable
Módulo Administración de Usuarios
Módulo Contable
Módulo Programación Financiera
En desarrollo por el Grupo "Soporte de Sistemas para Gestión Interna"
Compras y Contrataciones
Rendición Contable