UNIVERSIDAD DEL BIO-BIO

Facultad de Ciencias Empresariales

Departamento de Auditoria y Administración

MEMORIA PARA OPTAR AL GRADO DE CONTADOR PÚBLICO Y AUDITOR

PLAN DE CONTINGENCIA TIC PARA EL RESGUARDO DE INFORMACION ANTE EVENTUALIDADES EN EL SERVICIO PÚBLICO

ALUMNO: RODRIGO GARRIDO Y.

PROFESOR GUÍA: JUAN MALDONADO R.

CONCEPCION, 2014

AGRADECIMIENTOS

Primero que todo agradezco a Dios, por llevarme por el camino hacia la superación personal, a mis amados padres que siempre tuvieron una palabra de aliento y apoyo cuando las cosas no se veían muy bien, a mis profesores y profesor ayudante que pese a su agenda ocupada siempre estuvieron presentes orientándome hacia la obtención de las metas, aportando con su granito de arena para hacer de mi un profesional, por sus consejos y su palabra siempre acertada y alegre para cuando pensé que no podía.

Especialmente, quisiera agradecer a la mujer maravillosa que ha estado a mi lado, que siempre creyó en mí, aun cuando yo dude, la que me empujo a ser un mejor hombre, esposo y a crecer profesionalmente, que me contuvo cuando ya no daba más, que me apoyo incondicionalmente, y me levanto una y otra vez con una palabra de aliento, la que me sostuvo y me enseño a mirar siempre el lado positivo de la vida, que solo uno es el dueño de su futuro y que siempre puedes lograr tus sueños con perseverancia, empeño y dedicación, y que pese a lo oscuro que se vea el camino, siempre habrá una luz para guiarte, la luz de dios , mis padres, mis profesores y mi amada esposa.

INDICE

INDICE…….3

CAPITULO I…….6

1. INTRODUCCION……..…6

1.2 PLANTEAMINETO DEL PROBLEMA……..8

1.3 JUSTIFICACION……11

1.4 OBJETIVO GENERAL……..…….11

1.5 OBJETIVOS ESPECIFICOS……..……..…12

1.6 METODOLOGIA……13

1.6.1….MUESTRA ENTIDADES PUBLICAS……..13

CAPITULO II……15

2.1 MARCO CONCEPTUAL…….15

2.2 CONCEPTOS GENERALES…….15

2.2.1 SISTEMAS DE INFORMACION……..16

2.3 PLANES Y SUBPLANES……..19

2.4 . SEGURIDAD DE LA INFORMACION…….21

2.4.1 .ASPECTOS GENERALES SEGURIDAD DE INFORMACION…….22

2.4.1.1SEGURIDAD FISICA……..……..22

2.4.1.2SEGURIDAD LOGICA…….26

2.5 CONCEPTOS BASICOS……33

2.6 ESTANDARES Y BUENAS PRACTICAS……37

CAPITULO III……..…….44

3.1 PLAN DE CONTINGENCIA TI……..44

3.1.2 ETAPAS PARA ELABORAR UN PLAN DE CONTINGENCIA…….46

3.2 PLAN DE RECUPERACION ANTE DESASTRES……..…….49

3.2.1 ELEMENTOS CLAVE…….……50

CAPITULO IV……..55

4.1 AUDITORIA AL PLAN DE CONTINGENCIA……..55

4.1.1 TIPOS DE AUDITORIAS DE SISTEMAS…….....57

4.2 CHEQUEO DE AUDITORIA ……..58

CAPITULO V…….59

RESUSLTADOS……..……..……59

CONCLUSION……..……121

BIBLIOGRAFIA…….…….....125

LINKOGRAFIA…….……..126

ANEXOS……..….127

CAPITULO I

INTRODUCCIÓN

Desde tiempos inmemoriales el hombre, siempre ha estado ligado a la información y a la tecnología, desde el principio de su existencia, ha realizado acciones para modificar el medio que le rodea con la finalidad de satisfacer las necesidades que iban surgiendo. Como cita Donald Cardwell (1996) en su libro 'Historia de la Tecnología'

Dibujando en cuevas, escribiendo, en piedras, tablillas, pergaminos, papiros, libros, todo con el fin de mantener la información en el tiempo, para que otras generaciones pudiesen tener acceso a ella.

Con la información aparecieron las ciencias, se pudo observar y analizar y por medio de la Ciencia nace la Tecnología, la creación de herramientas y técnicas para un propósito practico. esta Tecnología parte en la Edad de Piedra, las primeras herramientas estaban asociadas a la supervivencia del hombre, en las Edades posteriores solo se dejo entre ver los avances de ella, posteriormente el hombre en base a toda esta información creo las civilizaciones, Egipto, Grecia, Roma, China, India. Incas y Mayas, algunas inexistentes, pero gracias al conocimiento, avances tecnológicos y escrituras, sobre ellas se les conoce, hoy en día. Posteriormente el hombre daría un gran salto con la revolución industrial que llevo todo este conocimiento al desarrollo de la sustentación, mediante la economía, conocida también como el conjunto de cambios tecnológicos y económicos, implicando en los procesos

productivos, que permitieron transformar la sociedad agrícola a la sociedad industrial (Avervuj y Martinez, Educación Tecnológica)

El descubrimiento de nuevos conocimientos permitió crear nuevas cosas y recíprocamente se han podido realizar nuevos descubrimientos científicos, gracias a esto nuestro desarrollo tecnológico a extendidos las fronteras posibilitando por ejemplo la experimentación, y la obtención de mas conocimiento.

Es por ello que no podemos pensar que el desarrollo tecnológico pertenece tan solo al presente y al futuro. No olvidemos que la tecnología es una actividad ligada al proceso de hominización y, por tanto, es tan antigua como nuestra existencia (San Martín, 1990; Cardwell, 1996; ITEA, 2000).

Sin embargo el desarrollo tecnológico no ha sido impedimento para la perdida de la información durante las distintas edades o eras, siempre ha existido un alto riesgo sobre ella la mantención y resguardo de estos conocimientos siempre se ha visto afectada, por una serie de factores, ya sea naturales como terremotos, inundaciones, incendios, guerras, y además por eventualidades como cortes de energía , o actuación de hacker, cracker, que vulneran la seguridad de las empresas con el fin de la sustracción, divulgación, y eliminación poniendo en riesgo a la organización ya sea privada o pública.

Por ende las Organizaciones invierten grandes cantidades de dinero con el fin de mantener segura la información, es así como nace un conjunto de medidas preventivas y reactivas para

mitigar las ocurrencias de hechos que vulneran la seguridad, se busca con ello resguardar, proteger y mantener la confidencialidad, disponibilidad e integridad de la misma, además esta seguridad involucra la implementación de estrategias que cubran los procesos donde la información es el activo primordial, estas estrategias deben poseer políticas y controles de seguridad y procedimientos para detectar amenazas que puedan explotar las vulnerabilidades que pongan en riesgo dicho activo por lo cual dicha seguridad incumbe a gobiernos, entidades militares, instituciones financieras y empresas privadas.

1.2 PLANTEAMIENTO DEL PROBLEMA

El crecimiento de las entidades públicas y/o privadas en chile y en el mundo, debido la rapidez en el desarrollo de las tecnologías, ha hecho que los sistemas de información se masifiquen en forma acelerada, convirtiéndose en un elemento clave, para la gestión de la organización.

Desde una mirada economista, si los recursos básicos a analizar hasta ahora eran tierra trabajo y capital, ahora la información aparece como otro insumo a valorar en las empresas y entidades transformándose así en el activo más importante de la organización. Pública y/o privada.

Con el crecimiento de los países, su información y la tecnología, crecieron también los riesgos asociados a ella, algunos intencionales y otros no, como perdida de información, robo y sustracción, modificación de esta y espionaje industrial, además de las eventualidades por cortes de energía, caídas del sistema y los riesgos que ya existían como terremotos,

incendios tsunamis e inundaciones que no solo limitan a las organizaciones en la entrega del servicio, también destruye su infraestructura. De todo esto surgen interrogantes:

¿Las entidades públicas de nuestra región cuentan con planes que aseguren la información?

¿Se encuentran preparadas ante eventualidades ya sean provocadas o no?,

¿En cuánto tiempo es posible recuperar la información?,

Mediante la investigación y el desarrollo de una propuesta de recuperación de información o plan de contingencia orientado a la entidad pública responderemos estas interrogantes.

1.3 JUSTIFICACIÓN DEL PROYECTO

El año 2007 el Ministerio del Interior, en su rol de Coordinador del Subcomité de Gestión de Seguridad y Confidencialidad de Documentos Electrónicos, detectó que en las instituciones del sector público persistían algunas falencias respecto de estos temas, entre las cuales se menciona: aplicaciones y sistemas informáticos con configuración inadecuada, sitios web de gobierno implementados deficitariamente y con vulnerabilidades conocidas, redes informáticas institucionales con debilidades en sus mecanismos de control de acceso y de regulación del tráfico de datos, problemas de continuidad operacional frente a incidentes de índole recurrente, como cortes de energía eléctrica, e inexistencia de políticas de seguridad institucionales.

En chile y el mundo no es difícil encontrar noticias sobre eventualidades o problemas ocasionados por el robo o sustracción de información y/o vulneración de los sistemas de seguridad Tic,

Recientemente el diario El Espectador, publico el día 21 de enero del 2014, la noticia sobre un trabajador de la empresa Corea Credit Bureaut, de corea del sur, quien sustrajo información financiera de tres grandes entidades, mediante memorias USB, sustrayendo los datos de más de 20 millones de personas, la cual fue vendida a empresas de mercadeo telefónico, la empresa en cuestión según un agente de ella confirmo que la sustracción de los datos se debió a la precaria seguridad de las firmas financieras.

Las entidades públicas de nuestro país no se encuentran ajenas a este tipo de eventualidades ya que la seguridad de sus sistemas de información puede ser violada inclusive desde el interior.

En chile el diario la tercera en su edición del 22/03/2014 publico, el robo de una base de datos del registro civil, el 30 de octubre del 2013, la directora de la entidad Claudia Gallardo, denuncio el hecho y pidió a la fiscalía norte indagar la extracción la cual se realizo mediante una copia de la base de datos que contenía registros 50.481.298 relativos a documentación de Cedula de identidad y pasaportes de todos los chilenos, por parte de un funcionario a honorarios del servicio, el cual fue desvinculado de la institución.

Pese a todo este tipo de vulnerabilidades, no existe una conciencia clara y precisa sobre los riesgos asociados a la información y su resguardo, la simple protección de los sistemas y la información no suele eliminar completamente la posibilidad de que estos sufran daños, debido a hechos fuera del alcance de la entidad y del hombre como son también las catástrofes naturales como terremotos, inundaciones, incendios provocados o no, en consecuencia los gestores deben implantar medidas de seguridad que lleven los riesgos a niveles aceptables, además de medidas para la recuperación de datos que permitan a la entidad continuar con su funcionamiento en el menor tiempo posible.

1.4 OBJETIVO GENERAL

Esta investigación tiene como objetivo general Desarrollar una propuesta de recuperación de información ante desastres, mediante un plan de contingencia TI, en entidades públicas. a través de estándares, buenas prácticas y/o guías.

Sabiendo que el resguardo de la información es primordial, también lo es su recuperación, además de la preparación de la entidad en el caso de ocurrencia de alguna de ellas, para su rápida puesta en marcha.

Para lo cual se desarrollaran entrevistas con el encargado del área TI de la organización, con el fin de verificar si esta cuenta con algún método de seguridad para protegerse. Además se desarrollará un diagnóstico mediante los estándares antes mencionados.

1.5 OBJETIVOS ESPECIFICOS

1. Determinar el grado o nivel de seguridad de la información en la entidad.

2. Determinar los principales y/o potenciales riesgos de pérdida de información ya sean provocados o no.

3. Determinar de entre los diferentes estándares de seguridad, el o los más apropiados para generar el desarrollo de la propuesta.

4. Establecer un plan de recuperación de información a nivel hardware, software.

METODOLOGIA

Diseño de estudio: estudio del tipo descriptivo

Objeto de estudio: Servicio público, estándares y guías, utilizados para el resguardo de información ante eventualidades.

Muestra: Entidades Públicas

Municipalidades de las comunas de Chiguayante, San Pedro de la Paz y Hualqui, además del Senda de la región del Bio Bio**.**

Instrumento recolector de datos:

- Entrevistas al personal clave: Encargado Área Informática de las Entidades Públicas. Las entrevistas serán realizadas al encargado del área TIC de cada Entidad evaluada.
- Diagnostico mediante check list

Diagnostico 1: Conocimientos planes de Contingencia, las preguntas están orientadas a cada fase del plan de contingencia.

Diagnostico 2: Conocimiento del sistema inventario de sistemas

Diagnostico 3: Conocimiento en seguridad física, lógica redes y sistemas, de conformidad a estándares.

Procedimiento: El proceso del estudio se llevará a cabo a través de las siguientes etapas:

- Análisis de la Entidad.

- Entrevistas con personal clave
- Aplicación check list.
- Conclusión estado entidades.
- Desarrollo propuesta.

CAPITULO II:

ASPECTOS GENERALES

MARCO CONCEPTUAL

Conceptos Generales

Es de vital importancia explicar la conceptualización básica, y la terminología que en el presente estudio se utiliza, con el objeto de profundizar en los temas asociados al plan de contingencia y recuperación de la información.

Tecnologías de la Información y la Comunicación

Según la Information Technology Association of America (Asociación Americana de las Tecnologías de la Información: ITAA) TIC (ITC en inglés) es "el estudio, el diseño, el desarrollo, el fomento, el mantenimiento y la administración de la información por medio de sistemas informáticos, esto incluye todos los sistemas informáticos no solamente la computadora, este es solo un medio más, el más versátil, pero no el único; también los teléfonos celulares, la televisión, la radio, los periódicos digitales, etc."

En pocas palabras, las Tecnologías de la Información tratan sobre el empleo de computadoras y aplicaciones informáticas para transformar, almacenar, gestionar, proteger, difundir y localizar los datos necesarios para cualquier actividad humana.

Sistemas de Información

Un sistema de información es un conjunto de elementos interrelacionados con el propósito de prestar atención a las demandas de información de una organización, para elevar el nivel de conocimientos que permitan un mejor apoyo a la toma de decisiones y desarrollo de acciones. (Peña, 2006).

En cuanto a los sistemas de información podemos señalar.

Otro autor define que "Un sistema de información es el sistema de personas, registros de datos y actividades que procesa los datos y la información en cierta organización, incluyendo manuales de procesos o procesos automatizados." (s/a, 2008).

Según Peralta Manuel (2008) un sistema de información es un conjunto de elementos que interactúan entre si con el fin de apoyar las actividades de una empresa o negocio, la cual realiza cuatro actividades básicas.

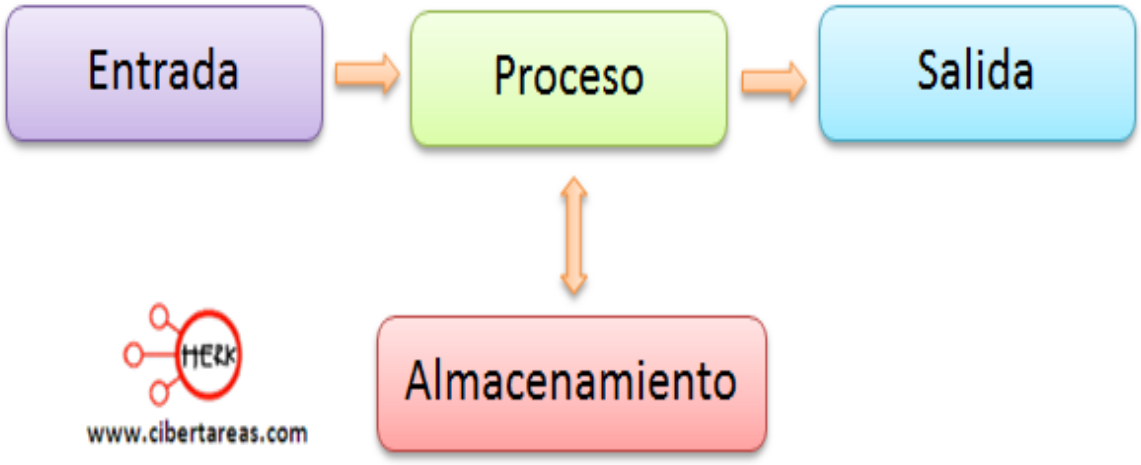
Entrada de Información: Es el proceso mediante el cual el Sistema de Información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o

automáticas. Las manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos. Esto último se denomina interfaces automáticas. Las unidades típicas de entrada de datos a las computadoras son las terminales, las cintas magnéticas, las unidades de diskette, los códigos de barras, los escáner, la voz, los monitores sensibles al tacto, el teclado y el mouse, entre otras

Almacenamiento de Información*:* El almacenamiento es una de las actividades o capacidades más importantes que tiene una Computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras de información denominadas archivos. La unidad típica de almacenamiento son los discos magnéticos o discos duros, los discos flexibles o diskettes y los discos compactos (CD-ROM).

Procesamiento de Información: Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados. Esta característica de los sistemas permite la transformación de datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general de un año base.

Salida de Información*:* La salida es la capacidad de un Sistema de Información para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, terminales, diskettes, cintas magnéticas, la voz, los graficadores y los plotters, entre otros. Es importante aclarar que la salida de un Sistema de Información puede constituir la entrada a otro Sistema de Información o módulo. En este caso, también existe una interface automática de salida.



Fuente: www.cibertareas.com

Además los Sistemas de Información según Peralta (2008) cumplen tres objetivos básicos dentro de las organizaciones.

1. **Automatización de procesos operativos***:* Lo Sistemas de Información que logran la automatización de procesos operativos dentro de una Organización o entidad, son

llamados Transaccionales, ya que su función primordial consiste en procesar transacciones tales como pagos, cobros, pólizas, entradas, salidas, etc.

2. **Proporcionar Información que sirva de apoyo al proceso de toma de decisiones***:* Los Sistemas de Información que apoyan en el proceso de toma de decisiones son los sistemas de soporte a la toma de decisiones, sistemas para la toma de decisión de grupo, sistemas expertos, de soporte a la toma de decisiones y sistema de información para ejecutivos.
3. **Lograr ventajas competitivas a través de su implantación y uso***:* Este tercer tipo de sistema, de acuerdo con su uso u objetivos que cumple, es el de los sistemas estratégicos, los cuales se desarrollan en las organizaciones con el fin de lograr ventajas competitivas, a través del uso de la tecnología de información.

Planes y Sub-planes

Plan de Continuidad del Negocio

Plan de Continuidad del Negocio (Business Continuity Planning - BCP) Es el proceso de desarrollar planes y procedimientos dentro de la organización con el propósito de responder ante un desastre o interrupción significativa del negocio, de forma tal que las operaciones críticas del negocio puedan continuar sus operaciones dentro de un límite aceptable de tiempo, de acuerdo a lo establecido por la gerencia general. Además puede ser definido como un conjunto formado por planes de actuación, planes de emergencia, planes financieros,

planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía.

Plan de Contingencia Tic

El plan de contingencia es una herramienta de gestión necesaria, que ayudará a que los procesos críticos de la empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados. Corresponde a una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, de organización de emergencia y de procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos. Este plan contiene las medidas técnicas, humanas y organizativas, para que la organización garantice la continuidad de la operación, esta herramienta requiere la identificación de aquellos sistemas de información y/o recursos TIC,s críticos que son susceptibles de riesgo de deterioro, violación o perdida ya sea por causa física o humana, con el propósito de estructurar y ejecutar procedimientos y asignar responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de esta en el menor tiempo posible.

Un plan de contingencia abarca tres sub planes los que determinan las contramedidas necesarias para cada instante en el tiempo, respecto a la ocurrencia de cualquier amenaza. Estos sub planes son:

Plan de respaldo: considera las contramedidas preventivas antes de que se concrete una amenaza.

Plan de emergencia: considera las contramedidas necesarias cuando se ha concretado una amenaza, o inmediatamente después. Su finalidad es minimizar los efectos adversos

Plan de recuperación: considera las medidas necesarias después de que se ha concretado y controlado una amenaza. Su finalidad es restablecer el estado de las cosas, al estado en que se encontraban antes de que se concretara la amenaza.

Plan de Recuperación ante Desastres

"Plan de recuperación ante desastres del inglés(*Disaster Recovery Plan*) es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos. Esto también debería incluir proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave, aunque esto no sea cubierto en este artículo, el propósito es la protección de datos".

Seguridad de la Información

"Son todas aquellas medidas preventivas y reactivas realizadas por el hombre, de las organizaciones y los sistemas tecnológicos que permitan resguardar y proteger la información mediante medidas como control de su uso, divulgación, alteración, modificación**,** lectura, registro o su destrucción**,** con el fin de mantener la confidencialidad, disponibilidad e integridad de la misma".

Aspectos Generales de la Seguridad de la Información

1. Seguridad Física

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos. Si se entiende la contingencia o proximidad de un daño como la definición de Riesgo de Fallo, local o general, tres serían las medidas a preparar para ser utilizadas en relación a la cronología del fallo. Plan de Contingencia de los Sistemas de Información," Antes, Durante, Después"

Antes

El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo o, en su caso, aminorar las consecuencias que dé él se puedan derivar tales como:

- Compartimentación.
- Elementos de la construcción.
- Ubicación del edificio.
- Potencia eléctrica.
- Sistemas contra Incendios.
- Control de accesos.
- Selección de personal.
- Seguridad de los medios.
- Medidas de protección.
- Duplicación de medios.

Durante

Se debe de ejecutar un plan de contingencia adecuado. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa.

La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la organización. Por otra parte, no es corriente que un negocio responda por sí mismo ante un acontecimiento como el que se comenta, se deduce la necesidad de contar con los medios necesarios para afrontarlo. Estos medios quedan definidos en el Plan de Recuperación de Desastres que junto con el Centro Alternativo de Proceso de Datos, constituye el plan de contingencia que coordina las necesidades del negocio y las operaciones de recuperación del mismo.

Son puntos imprescindibles del plan de contingencia:

• Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas

• Establecer un periodo crítico de recuperación, en la cual los procesos debe de ser reanudados antes de sufrir pérdidas significativas o irrecuperables.

• Realizar un Análisis de Aplicaciones Críticas por que se establecerán las prioridades del proceso.

• Determinar las prioridades del proceso, por días del año, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre.

• Establecer objetivos de recuperación que determinen el período de tiempo (horas, días, semanas).

• Designar entre los distintos tipos existentes, un Centro Alternativo de Proceso de Datos.

• Asegurar la capacidad de las comunicaciones.

• Asegurar la capacidad de los servidores back-up.

Después

Los contratos de seguros vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades que se puedan derivar para el centro de proceso de datos una vez detectado y corregido el fallo. De la gama de seguros existentes, se pueden indicar los Siguientes:

• Centros de proceso y equipamiento: se contrata la cobertura sobre el daño físico en el CPD (Centro de Procesamiento de Datos) y el equipo contenido en el.

• Reconstrucción de medios de software: cubre el daño producido sobre medios software tanto los que son de propiedad del tomador de seguro como aquellos que constituyen su responsabilidad.

• Gastos extra: cubre los gastos extra que derivan de la continuidad de las operaciones tras un desastre o daño en el centro de proceso de datos. Es suficiente para compensar los costos de ejecución del plan de contingencia.

• Interrupción del negocio: cubre las pérdidas de beneficios netos causadas por las caídas de los medios informáticos o por la suspensión de las operaciones.

• Documentos y registros valiosos: Se contrata para obtener una compensación en el valor metálico real por la pérdida o daño físico sobre documentos y registros valiosos no amparados por el seguro de reconstrucción de medio software.

• Errores y omisiones: proporciona protección legal ante la responsabilidad en que pudiera incurrir un profesional que cometiera un acto, error u omisión que ocasione una pérdida

Financiera a un cliente.

• Cobertura de fidelidad: cubre las pérdidas derivadas de actos deshonestos o fraudulentos cometidos por empleados.

• Transporte de medios: proporciona cobertura ante pérdidas o daños a los medios transportados.

• Contratos con proveedores y de mantenimiento: proveedores o fabricantes que aseguren la existencia de repuestos y consumibles, así como garantías de fabricación.

2. Seguridad Lógica

Se define como la arquitectura que se conforma por: software de antivirus, herramientas de respaldo, de revisiones de la infraestructura de red, enlace de telecomunicación, firewall, soluciones de autentificación, servicios de seguridad en vivo.

El propósito de la Seguridad Lógica es proteger la información y los activos de la organización, tratando de conseguir integridad, disponibilidad y confidencialidad de los datos y las responsabilidades que debe asumir cada trabajador.

Como por ejemplo:

- Restringir el acceso a los programas y archivos
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.

Elementos que conforman la seguridad lógica

Control de Acceso: Principal objetivo es controlar el acceso a la información, restringir la cantidad de usuarios y que solo ingrese personal autorizado.

Identificación y Autentificación: Esta etapa es el principal filtro para proteger el sistema, por ello la importancia, esto permite denegar el acceso al personal no autorizado

Identificación: Este proceso asegura que el sujeto (usuario, programa o proceso) es la entidad que dice ser, la identificación puede ser verificada con el uso de una credencial como un user name, personal identification number(PIN), smart card, firma digital, números de cuentas o atributos anatómicos

Autentificación*:* Es cuando la persona se acredita quien dice ser. Para este proceso se destacan cuatro formas donde el usuario puede realizar una autentificación de su identidad, de las cuales se aconseja hacer dos de las cuatros para obtener un grado aceptable de seguridad:

1. Algo que solamente la persona sabe: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número personal como una PIK, etc.
2. Algo que la persona posee: como una tarjeta magnética
3. Algo que el individuo es y que lo identifica naturalmente, la huella digital, escaneo de la palma, escaneo de iris, escaneo de retina etc.
4. Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura, como la firma

Transacciones*:* Aquí se pueden manejar los cambios de estado del sistema, ya que las transacciones están compuestas por varios procesos que se han de aplicar uno después de otro. En esta etapa se pueden implementar controles a través de mecanismos estándar para manejar los cambios como por ejemplo cada transacción poseerá una clave que la distinguirá del resto, y se sabrá que usuario la utilizó o realizó el cambio.

Limitaciones a los Servicios: Las limitaciones son controles de restricción que detendrá un proceso dependiendo de los parámetros propios de la utilización de las aplicaciones.

Modalidades de Acceso*:* Las modalidades de acceso son las formas de entrada que permiten al usuario ingresar sobre los recursos y a la información. Estas pueden ser:

- Escritura: Este tipo permite al usuario agregar datos, modificar o borrar información.
- Lectura: El usuario puede solamente leer o visualidad la información pero no puede alterarse. Debe establecerse si es que la información puede ser copiada o impresa.
- Ejecución: Este acceso se caracteriza por otorgar al usuario privilegios de ejecutar distintos programas o aplicaciones.
- Eliminar: Permite al usuario borrar recursos del sistema.
- Todas las anteriores.
-

Modalidades de acceso especiales*:*

- Creación: Entrega al usuario los permisos para crear nuevos registros, campos y archivo.
- Búsqueda: permite enumerar, registrar, inventariar los archivos de un directorio determinado.

Ubicación y Horario: Este tipo de control puede ser clave en la seguridad de la información por que determina los accesos a ciertos recursos de los sistemas tanto en su ubicación física o lógica de los datos de personas.

Los horarios son tipo de controles que permiten acotar, localizar, restringir los accesos de usuarios a determinadas horas, días, meses, años. Con esto se busca mantener un control limitado de los usuarios y los lugares de ingreso.

Se debe destacar que estos dos controles deben ser siempre acompañados de algunos de los controles antes mencionados para su óptimo funcionamiento.

Control de Acceso Interno

Palabras Claves (Passwords): Las password son utilizadas generalmente para realizar autenticación del usuario y sirve para proteger los datos y aplicaciones de los programas de información. Estos tipo de controles resultan de muy bajo costo para la organización, de esta forma se recomienda implementarlo. Pero el problema de las palabras claves es cuando los usuarios se ven en la necesidad de utilizar varias passwords para acceder a varios sistemas ya que optará por utilizar la misma

Passwords Uniformes (Sincronizar): Esto se trata de permitir que el usuario tenga acceso con la misma passwords a diferentes sistemas interrelacionado, lo que permitirá la actualización automática en todos ellos en caso de ser modificados

Término y Control*:* Este mecanismo controla cuando pueden o deben cambiarse las claves de los usuarios. Las passwords tendrá un periodo mínimo para que el usuario pueda cambiar y un periodo máximo que puede transcurrir para que estas caduquen.

Las passwords que existan en la empresa deben tener una longitud mínima de 6 caracteres y una longitud máxima de 10 caracteres, numéricos o alfanuméricos.

Los cambios en los password la hacen los usuarios a través de la cuenta, allí hay una opción para realizar la modificación. **Se recomienda que el usuario cambie más de una ves por año ya que ese es el plazo de expiración de la password.**

Encriptación: La encriptación es un proceso donde se vuelve ilegible la información que se considera importante. Esta medida de seguridad es usada para almacenar o transmitir información que debe ser confidencial.

El tipo de información encriptada solo puede ser desencriptada por quienes posean la clave apropiada, esto puede ser potente medida de control de acceso.

Lista de control de acceso*:* Este tipo de control se trata de un registro donde se halla los nombres de los usuarios que cuentan con la autorización para acceder a los recursos del sistema. Esto se podrá ejecutar dependiendo del número de usuarios por su capacidad.

Limites Sobre la Interfaz de Usuario*:* Este control generalmente es utilizado en un conjunto de nóminas de control de acceso y registra a los usuarios que realizarán funciones específicas. Estos límites se pueden implementar en:

- Menús
- Vistas sobre la Base de Datos
- Límites físicos sobre la interfaz de usuario

Etiqueta de Seguridad*:* Las Etiquetas de Seguridad se adhieren a un objeto a proteger con el fin de que no sean abiertas o violadas. En caso de apertura se destruyen y deja una marca en la superficie del objeto indicando la violación del mismo.

Control de Acceso Externo

Dispositivos de Control de Puertos*:* Este instrumento autoriza el acceso a un puerto determinado y puede estar físicamente separado o incluir en otros dispositivos de comunicación. (Ejemplo un modem)

Firewalls o Puertas de Seguridad*:* Este dispositivo permite bloquear o filtrar el acceso no autorizado, este puede ser configurado para permitir, limitar, cifrar, descifrar, el tráfico entre la información de un determinado sistema, dependiendo de normas y otros criterios.

Principalmente los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectada a Internet como por ejemplo la intranet de la organización. Todos los mensajes que entren o salgan de la intranet pasan a través de los cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen con los criterios de seguridad.

Este tipo de control permite que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización.

Acceso de Personal Contratado o Consultores*:* Para este tipo de personal debe ponerse especial atención en las políticas y procedimientos administrativos, ya que ellos estarán temporalmente en la organización, debiéndose proteger la información. Por tanto, solo accederán a la información necesaria para efectuar su trabajo y solo se le dará acceso por el tiempo que se encuentre trabajando dentro de la empresa.

Accesos Públicos*:* Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

Administración: Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas, es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

La clasificación deberá realizarse en base a una identificación individual del contenido de las bases de datos y determinando la importancia para la continuidad del negocio, considerando las consecuencias de pérdidas, divulgación o acceso indebido.

De esta manera se estima la siguiente clasificación para la información:

- Confidencial: información estratégica o de reserva absoluta.
- Uso Restringido: uso restringido para un grupo de la gerencia y/o jefaturas de áreas.
- Uso interno: utilizadas por los funcionarios de la empresa.
- Uso público: es utilizada por clientes, proveedores u otros.

Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

También debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.

Administración del Personal y Usuarios - Organización del Personal

Este proceso lleva generalmente cuatro pasos:

1. Definición de puestos
2. Determinación de la sensibilidad del puesto
3. Elección de la persona para cada puesto
4. Entrenamiento inicial y continuo del empleado

Este proceso debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

También se recomienda contar con un "Administrador de Base de Datos" (DBA) que será el encargado de crear la base de datos en sí y poner en vigencia los controles técnicos necesarios para apoyar las políticas dictadas por el administrador de datos. El Administrador de Base de Datos se encarga también de garantizar el funcionamiento adecuado del sistema y de proporcionar otros servicios de índole técnica relacionados.

Objetivos del Administrador de la Base de Datos.

- Mantener la Integridad, Seguridad y Disponibilidad de los Datos.

El DBA es responsable principalmente de:

- Administrar la estructura de la Base de Datos
- Administrar la actividad de los datos
- Administrar el Sistema Manejador de Base de Datos
- Establecer el Diccionario de Datos
- Asegurar la confiabilidad de la Base de Datos

Confirmar la seguridad de la Base de Datos de esta manera la seguridad de la información estará mejor resguardada ya sea por el Administrador de la base de datos quien creara las restricciones para la administración de la información, como por el Auditor Interno, que seguirá los procesos o actividades que los usuarios realicen.

Conceptos básicos

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

Integridad: Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc. Plan de Contingencia de los Sistemas de Información

Base de Datos*:* Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System- DBMS).

Las características que presenta un DBMS son las siguientes:

• Brinda seguridad e integridad a los datos.

• Provee lenguajes de consulta (interactivo).

• Provee una manera de introducir y editar datos en forma interactiva.

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

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

Criticidad: Característica que se fundamenta entre otras variables, en el nivel del Riesgo y en su importancia estratégica

Ataque: Acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

Ataque Activo*:* Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal.

Ataque Pasivo*:* Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red.

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

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

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

Riesgo: (Ingles: Risk*)*. Posibilidad que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información, suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Desastres: Los desastres son eventos extraordinarios que originan destrucción considerable de bienes materiales y pueden dar por resultado muerte, lesiones físicas y sufrimiento humano. Estos sucesos pueden ser causados por el hombre o naturales

Tiempo Máximo de Interrupción*:* Lapso de tiempo (horas hábiles) en el cual el proceso y los servicios de TI deben ser restaurados a un nivel operacional aceptable.

Vulnerabilidad*:* Debilidad de un activo o control que puede ser explotada por una o más amenazas

Impacto: Daños ocasionados a la empresa, como resultado del ataque de una amenaza a la vulnerabilidad del sistema. Por lo general, es cuantificada en unidades monetarias o por pérdidas ocasionadas

Mitigación: Medidas de intervención dirigidas a reducir o atenuar el riesgo. La mitigación es el resultado de una decisión política y social en relación con un nivel de riesgo aceptable, obtenido del análisis del mismo y teniendo en cuenta que dicho riesgo es imposible de reducir totalmente.

Recuperación: Proceso de restablecimiento de condiciones adecuados y sostenibles de vida mediante la rehabilitación, reparación o reconstrucción del área afectada, los bienes y

servicios interrumpidos o deteriorados y la reactivación o impulso del desarrollo económico y social de la comunidad.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas).

Estándares y Buenas Prácticas

Un estándar es un documento establecido por consenso, aprobado por un cuerpo reconocido y que ofrece reglas, guías y/o características para que pueda usarse repetidamente, los estándares proveen las guías especificas de las mejores prácticas a los directores de proyecto programas y portafolios, así como a sus organizaciones, ahorrando la creación de soluciones constantes para un problema determinado

El organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica, es la **International Organization for Standardization (ISO).** Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.

ISO 27001/IEC (Information technology - Security techniques - Information security management systems – Requirement

Es un estándar para la seguridad de la información denominado ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) adoptado por ISO, basado en un estándar británico denominado BS 7799. Es certificable y su primera publicación fue en el año 2005.

ISO/IEC 27002 (Information Technology-Security-Techniques-Code of Practice for Information Segurity-Management).

Es una guía de buenas prácticas a partir de objetivos de control y controles recomendables a nivel de seguridad de la información. A diferencia de ISO 27001, no es un estándar certificable. Cuenta con 39 objetivos de control y 133 controles agrupados en 11 dominios, abordando más controles y dominios que los establecidos en el estándar certificable ISO 27001.

ISO/IEC 27005 (Information technology — Security techniques — Information security risk management)

Se trata de un estándar internacional denominado ISO 27005, creado el año 2008, que provee pautas para la gestión de riesgos de seguridad de la información.

Al hablar de seguridad de la información, aparece el análisis, evaluación y gestión de los riesgos por ende este documento ilustra un marco de referencia para su tratamiento.

ISO/IEC 27035 (Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad)

Publicada el 17 de Agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información

Este estándar hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades

Buenas Prácticas en seguridad de sistemas de información

En general el concepto de "buenas prácticas" se refiere a toda experiencia que se guía por principios, objetivos y procedimientos apropiados o pautas aconsejables que se adecuan a una determinada perspectiva normativa o a un parámetro consensuado, así como también toda experiencia que ha arrojado resultados positivos, demostrando su eficacia y utilidad en un contexto concreto, tales como:

ISACA (Information-Sistems-Audit-and-Control.Asociacion) Asociación de Auditoría y Control de Sistemas de Información. Asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de Auditorías y control en sistemas de información, tales como:

COBIT4.1

Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objetives for Information and related Technology) es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información (TI). Mantenido por ISACA (en inglés: Information Systems Audit and Control Association) y el IT GI (en inglés: IT Governance Institute)

En su cuarta edición, COBIT tiene 34 procesos que cubren 210 objetivos de control (específicos o detallados) clasificados en cuatro dominios:

Planear y organizar.

Adquirir e implementar.

Entregar y dar soporte.

Monitorear y evaluar.

Estándar para la Gestión de Servicios Informáticos, ITIL

La Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) fue desarrollada en 1980 por la CCTA (Agencia Central de Telecomunicaciones), buscando estandarizar la operación de todos los proveedores de tecnología (internos y externos) para el gobierno del Reino Unido. El resultado fue una guía que está formada por una serie de "Mejores prácticas" procedentes de todo tipo de suministradores de servicios de TI.

ITIL especifica un método sistemático que garantiza la calidad de los servicios de TI.

Ciclo de vida ITIL

Fuente: http://www.secureit.es/wp-content/uploads/2013/03/itil.png

El ciclo de vida ITIL, consta de cinco fases,

Estrategia del servicio:

Esta fase del ciclo de vida ITIL, define directrices para el diseño, desarrollo e implantación de la gestión del servicio como un recurso estratégico. Es fundamental en el contexto de los procesos que se siguen en las otras fases del ciclo de vida del servicio. Su principal función es mejorar la sincronización entre TI y las estrategias empresariales.

Diseño del servicio:

Se ocupa del diseño y desarrollo de servicios y sus procesos relacionados. Afecta tanto a los nuevos servicios, como a los que han sido modificados. Entre sus objetivos están: contribuir con los objetivos del negocio, ahorrar (en lo posible) tiempo y dinero, minimizar riesgos y evaluar y mejorar la eficiencia de los servicio de TI.

Transición del servicio:

Convierte las especificaciones de la fase anterior, en un servicio nuevo o modificado, reduciendo las variaciones en el rendimiento y los errores conocidos y garantizando que este cumple con los requisitos del negocio. Para lograr esto, se vale de los siguientes pasos: planificación y preparación, construcción y pruebas, pilotos, y planificación y preparación del despliegue

Operación del servicio:

Tiene como objetivos la coordinación y ejecución de las actividades y procesos necesarios para entregar y gestionar servicios para usuarios y clientes con el nivel especificado. También tiene la responsabilidad de gestionar la tecnología necesaria para la prestación y el soporte de los servicios.

Mejora continua del servicio:

Se centra en las actividades que mejoran la calidad del servicio. Para esto utiliza el ciclo "Planear, hacer, verificar actuar", que establece una fase de consolidación para cada mejora,

con el fin de incorporar nuevos procedimientos en la organización. Las medidas y análisis son muy importantes, ya que permiten identificar los servicios rentables y aquellos que se pueden mejorar.

CAPITULO III

3.1 PLAN DE CONTINGENCIA TI

INTRODUCCION

Toda organización debe planear y desarrollar un Plan de Contingencia cuando todavía no es necesario, es decir**,** ante**s** de que los eventos ocurran. La planificación aumenta la habilidad y capacidad de la organización para "sobrevivir" y mantener las operaciones en caso de incidentes o desastres, sirviendo como punto de partida y aportando una guía de acciones que se deben ejecutar para una adecuada respuesta en caso de emergencia.

El Plan de Contingencia debe cubrir todos los aspectos que se van a adoptar tras una

Interrupción, lo que implica suministrar el servicio alternativo y para lograrlo no solo se deben revisar las operaciones cotidianas, sino que también debe incluirse el análisis de los principales componentes de la infraestructura en riesgo. Esto incluye cubrir los siguientes puntos: hardware, software, documentación, talento humano y soporte logístico; debe ser lo más detallado posible y fácil de comprender. Los responsables de la planificación, deben evaluar frecuentemente los planes creados, así como analizar otras situaciones que se pudieran llegar a presentar. Un Plan de Contingencia estático se queda rápidamente obsoleto y produce una falsa sensación de seguridad, por lo cual debe ser un documento "vivo", actualizándose, corrigiéndose, y mejorándose constantemente, de manera que se pueda confiar en que las medidas adoptadas son apropiadas y pertinentes. También es necesario considerar como será divulgado.

Un Plan de Contingencia debe ser exhaustivo, evitando entrar en demasiados detalles;

Debe ser de fácil lectura, cómodo de actualizar, y debe ser una guía operativa clara y precisa. En síntesis, debe decir qué hay que hacer, quién, cuándo y cómo. El Plan de Contingencia debe tener en cuenta al personal que participa en su Implementación y aquellos que participarán operativamente en el momento en que se presente un incidente y el plan deba ejecutarse. Este debe detallar los nombres de los encargados de la contingencia y sus responsabilidades

Objetivos del Plan de Contingencia

Un plan de contingencia debe considerar distintos factores, a medida que se desarrolla el plan, por lo que los factores a considerar son:

- Debe estar preparado para alguna interrupción o desastre, por lo que debe ser capaz de dar respuesta a todos los incidentes que puedan afectar los procesos críticos de la organización
- Procedimientos para declarar un desastre
- Circunstancias bajo las cuales se debe declarar un desastre, ya que cualquier interrupción no representa un desastre. Si se debe considerar que un incidente por pequeño que sea, es capaz de convertirse en un desastre si no es manejado de manera oportuna y en el momento oportuno
- Procedimientos de evacuación
- Identificación de las responsabilidades en el plan

- Identificación de las personas responsables de cada función del plan
- Identificación de información de los contratos
- Identificación detallada de los pasos a seguir para la recuperación
- Clara identificación de los recursos necesarios para la recuperación y operación continua de la organización
- Aplicación paso a paso de la etapa de recuperación

Etapas para la Elaboración de un Plan de Contingencia de los Sistemas de Información

Etapas básicas para la elaboración de un Plan de Contingencia.

Todo Plan de contingencia de los sistemas de información, debe constar con un análisis y valoración de riesgos (impacto que causaría en la organización una falla e incidente en la plataforma tecnológica, o un desastre natural), identificando los procesos críticos y las consecuencias que se presentaría al no estar en funcionamiento dicho plan.

Esta evaluación tiene como fin:

- Determinar la relación costo beneficio y tener argumentos para la decisión del valor de la pérdida de.
- Clasificar los componentes de la plataforma tecnológica en términos de riesgo ya sean Altos, Medios, Bajos,.
- Cuantificar el impacto en caso de suspensión del servicio ya sea por minutos y horas.
- Determinar el grado y valor de la información, con el fin de determinar cuál de ella representaría una mayor pérdida para la organización,

Dentro de las prioridades podemos decir que una buena evaluación del riesgo minimizara la ocurrencia de pérdidas de información.

También debe contar con una Jerarquización de aplicaciones, ósea se debe definir con antelación cuales son las aplicaciones primordiales para la organización, teniendo en cuenta que para cada departamento o área funcional de la organización, su operación es primordial y la más importante, la jerarquización debe estar avalada y respaldada por un comité de contingencia o por la alta dirección, procurando objetividad y minimizando el conflicto de intereses. el plan debe incluir una lista de los sistemas, aplicaciones y prioridades, así como identificar aquellos elementos informáticos (hardware, software base, software de aplicaciones, telecomunicaciones) que puedan ser críticos ante cualquier incidente o desastre, jerarquizándolos de acuerdo al orden de importancia dentro de la organización. Se deben incluir los problemas generados por ausencia de fuentes de energía, mala administración o uso de dispositivos de backup o cualquier otro daño de origen físico que pueda provocar la pérdida masiva de información.

Otro punto primordial es el establecimiento de requerimientos de recuperación, la cual busca determinar lo que se debe hacer para lograr una óptima solución, especificando las funciones con base en el estado actual de la organización.

Para ello es necesario realizar las siguientes actividades:

- profundizar la definición del problema,
- analizar áreas o componentes problema, comunicaciones y sus flujos,
- formulación de medidas de seguridad necesarias dependiendo del nivel de seguridad requerido,
- justificación del costo de implantar las medidas de seguridad, análisis y evaluación del plan de contingencia actual (si lo hay),
- determinar los recursos humanos, técnicos y económicos necesarios para desarrollar el plan,
- definir un tiempo prudente y viable para lograr que el sistema se libere y pueda entrar en operación.

Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar éste ante eventualidades que se puedan presentar con posterioridad.

Se debe tener presente que el plan de contingencia no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la empresa.

Para garantizar el éxito del plan de contingencia es conveniente que en su elaboración participen la alta dirección de la organización, personal técnico y operativo de los procesos y los usuarios, ya que los recursos necesarios para la puesta en marcha del plan, demandan mucho esfuerzo técnico, económico y organizacional y se requiere observar el sistema, la plataforma tecnológica y la operación de la compañía desde diversos puntos de vista.

También es necesario definir y generar simulaciones que permitan poner a prueba el plan de contingencia, el personal y los recursos necesarios para su realización. El propósito es intentar valorar el impacto real de un problema dentro de los escenarios establecidos como posibles.

En caso de que los resultados obtenidos difieran de los esperados, se debe analizar si el resultado varió por un problema en el ambiente de pruebas del plan, en cuyo caso se podrá corregir el problema y repetir la prueba, ó si el plan tiene vacíos o carencias en su definición. Es indispensable la capacitación y participación del equipo de contingencia para detectar y evidenciar posibles carencias del plan, así como una buena documentación para facilitar la ejecución de las pruebas.

La documentación del plan demanda un esfuerzo significativo, pero esta ayudará a comprender otros aspectos del sistema y puede ser apoyo para la empresa en caso de ocurrir un incidente o desastre. Debe incluir los procedimientos detallados que expliquen el paso a paso de las tareas de instalación y recuperación necesarias, procurando que sean entendibles y fáciles de seguir.

La documentación del plan de contingencia se debe desarrollar a medida que se avanza en la definición del plan y desde el mismo momento que nace, pasando por todas sus etapas; en ningún caso se debe dejar de lado esta labor, esperando a realizarla cuando se concluyan las pruebas y su difusión, pues se correría el riesgo de que la documentación resulte inexacta, difusa y que cualquier aspecto importante se pase por alto.

Con el plan de contingencia probado y documentado, surge la necesidad de su difusión y capacitación entre las personas encargadas de llevarlo a cabo. El mantenimiento del plan comienza con una revisión del plan existente y se examina en su totalidad realizando los cambios en la información que pudo haber ocasionado una variación en el sistema y realizando los cambios que sean necesarios. La generación del plan no muere aquí, por el contrario es el inicio de un ciclo de revisión, ajuste y divulgación constante que suministre a la organización la tranquilidad de estar preparada y lista ante cualquier incidente.

PLAN DE RECUPERACION ANTE DESASTRE

INTRODUCCION:

La creciente dependencia a los datos en la era de la información, los ha hecho el activo más valioso de la organización y/o compañía, señala Fernando Mollon, VP de VMware Latinoamericana, a medida que la infraestructura de TI aumenta también lo hace su complejidad, la importancia de la recuperación ante desastre crece, la interrupción del servicio o la perdida de información tiene un impacto critico en las finanzas de cualquier organización ya sea privada o pública, y por lo tanto el Disaster Recovery Plan (Plan de Recuperación ante Desastres o DRP, por sus siglas en ingles, se vuelve cada vez más relevante.

Pero como determinar qué tipo de plan necesitan las organizaciones, según el ejecutivo de VMware, cada plan debe ser personalizado según las necesidades de la organización y debe contemplar factores tales como el tipo de negocio o actividad, nivel de seguridad necesario para los datos y aplicaciones y ubicación entre otros elementos.

Elementos Esenciales para un Plan Solido de Recuperación ante desastres

Definición del plan

Para que un plan de recuperación ante desastres funcione, tiene que involucrar a la gerencia. Ellos son los responsables de su coordinación y deben asegurar su efectividad. Adicionalmente, deben proveer los recursos necesarios para un desarrollo efectivo del plan. Todos los departamentos de la organización participan en la definición del plan.

Establecimiento de prioridades

A continuación, la organización debe preparar un análisis de riesgo y crear una lista de posibles desastres naturales o causados por errores humanos, y clasificarlos según sus probabilidades. Una vez terminada la lista, cada departamento debe analizar las posibles consecuencias y el impacto relacionado con cada tipo de desastre. Esto servirá como referencia para identificar lo que se necesita incluir en el plan. Un plan completo debe considerar una pérdida total del centro de datos y eventos de larga duración de más de una semana.

Una vez definidas las necesidades de cada departamento, se les asigna una prioridad. Esto es importante, porque ninguna compañía tiene recursos infinitos. Los procesos y operaciones son analizados para determinar la máxima cantidad de tiempo que la organización puede sobrevivir sin ellos. Se establece un orden de recuperación según el grado de importancia. Esto se define como el Recovery Time Objective, Tiempo de Recuperación o RTO. Otro término importante es el Recovery Point Objective, Punto de Recuperación o RPO.

Selección de estrategias de recuperación

En esta etapa se determina las alternativas más prácticas para proceder en caso de un desastre. Todos los aspectos de la organización son analizados, incluyendo hardware, software, comunicaciones, archivos, bases de datos, instalaciones, etc. Las alternativas a considerar varían según la función del equipo y pueden incluir duplicación de centros de datos, alquiler

de equipos e instalaciones, contratos de almacenamiento y muchas más. Igualmente, se analiza los costos asociados.

Al momento de definir la estrategia de recuperación apropiada se debe considerar los resultados obtenidos en el análisis del impacto del negocio, el cual entrega el objetivo de tiempo de recuperación y objetivo de punto de recuperación, que son parámetros para poder definir las estrategias de recuperación óptimas para la organización.

Objetivo de tiempo de Recuperación: Este parámetro, determina el tiempo improductivo aceptable que tiene una organización, en el caso de una interrupción de sus operaciones. Este indica, el punto más anticipado en el tiempo en el que las operaciones de negocio deben ser retomadas después de un desastre.

Objetivo de punto de Recuperación: Este parámetro, determina la pérdida aceptable de datos de una organización, en el caso de una interrupción de sus operaciones. Este cuantifica efectivamente, la cantidad permitida de pérdida de datos en el caso de una interrupción, pero se debe tener presente que es casi imposible recuperar la totalidad de la información.

Fuente: www.consultinginformationtechnology.com

En una encuesta de 95 compañías realizada por la firma Sepaton en 2012, 41% de los encuestados reportó que su estrategia de DRP consiste en un centro de datos configurado activo-pasivo, es decir toda la información está respaldada en un centro de datos completamente configurado con la información crítica replicada en un sitio remoto. El 21% de los participantes utiliza una configuración activa-activa donde toda la información de la compañía se mantiene en dos o más centros de datos. El 18% dijo que usan aún cintas de respaldo; mientras que el 20% restante no tiene o no está planeando una estrategia todavía.

Para VMware, la vitalización representa un avance considerable al aplicarse en el Plan de Recuperación ante Desastres (DRP). Según la encuesta de Acronis, las razones principales por las que se adopta la virtualización en un DRP son: eficiencia mejorada (24%); flexibilidad y velocidad de implementación (20%) y reducción de costos (18%).

Alternativas de estrategias de recuperación

Existen varias alternativas de estrategias, pero su elección dependerá del tiempo mínimo que se tenga como objetivo para la recuperación de los sistemas y en función a la disponibilidad que entreguen los centros. Entre las alternativas se encuentran:

1. **Hot site:** son sitios de respaldo, que tienen una imagen espejo virtual del centro de datos de la organización, con todos los sistemas configurados y esperando solamente por los últimos respaldos de los datos de sus usuarios, desde las facilidades de almacenamiento fuera del sitio. Los Hot site, son recomendados para organizaciones en la cuales su tiempo de ruptura no supera las 24 a 48 horas.
2. **Cold site:** son sitios que tienen solo el ambiente básico, para realizar una instalación de proceso de información, como el cableado eléctrico, aire acondicionado, piso, entre otros. Estos sitios, están listos para recibir los equipos, pero no ofrecen ningún

componente en el lugar, antes que se requiera su uso. La activación del lugar puede llevar varias semanas.

3. **Warm site:** son sitios, que están parcialmente configurados, por lo general con conexiones de red y equipo periférico seleccionado, como por ejemplo unidades de disco y otros controladores, pero sin la computadora principal. El supuesto detrás del concepto de warm site, es que la computadora puede obtenerse rápidamente para una instalación de emergencia y como la computadora es la unidad más cara , dicho acuerdo es menos costoso que un hot site. Después de la instalación de los componentes el sitio puede estar listo para el servicio dentro de unas horas.

4. **Mirror site:** son servidores que tienen exactamente los mismos datos, pero ubicados físicamente en distintos lugares, y que en el caso de fallar uno de los servidores, el otro es capaz de mantener operando el sistema, sin perder información o sin interrumpir al usuario.

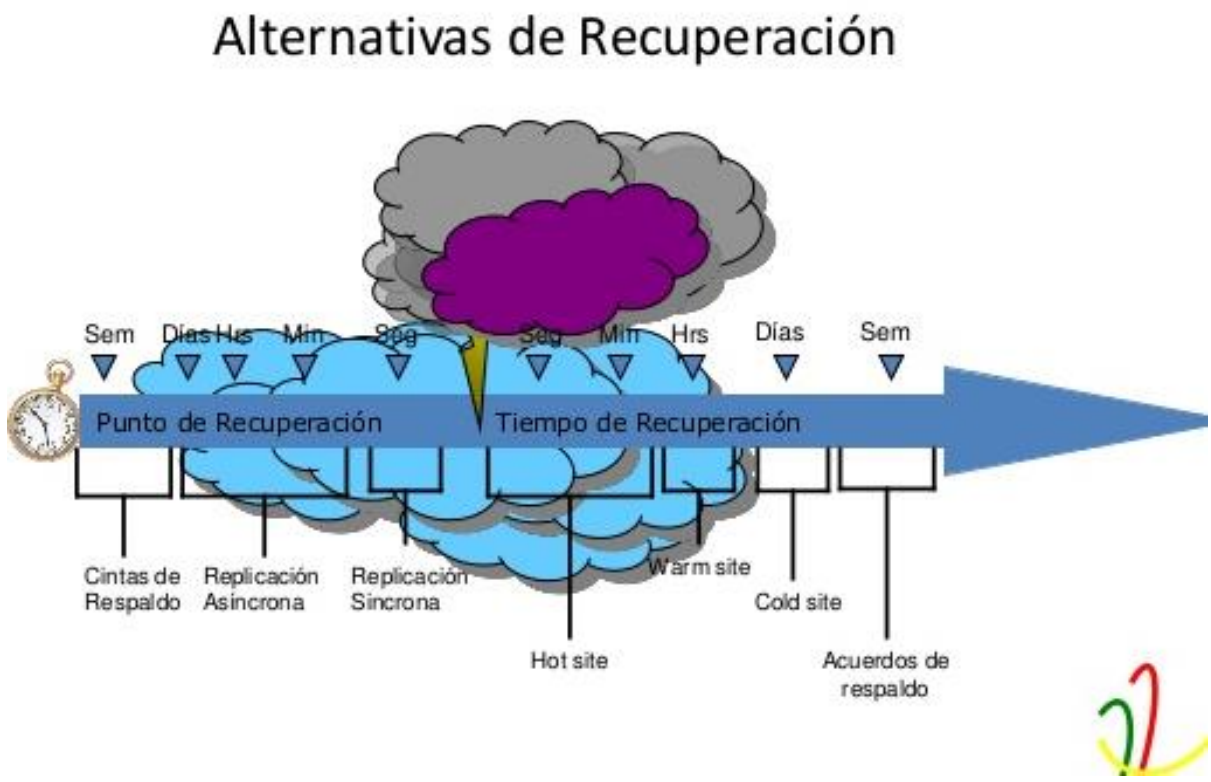
5. **Acuerdos recíprocos:** son acuerdos entre dos o más organizaciones, con equipo o instalaciones similares, el cual prometen proveerse mutuamente de tiempo de procesamiento, en caso de alguna emergencia.

6. **Sitios móviles:** estos sitios, son un remolque especialmente diseñado que puede ser transportado rápidamente a un lugar de negocio o a un sitio alterno, para proveer una instalación acondicionada y lista para el procesamiento de información. Estos sitios son una alternativa útil, cuando no hay instalaciones de recuperación en el área geográfica inmediata.

7. **Modalidad externa:** son acuerdos mediante un convenio con otra institución que posee equipos similares o mayores y que brindan la seguridad de poder procesar la información de la organización, y ser puestas a disposición de ella, en caso de producirse alguna interrupción o desastre, y mientras se busca una solución definitiva.

Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las organizaciones.

8. **Modalidad interna:** Si la organización posee más de un local, es necesario que en ambos esté señalado, los equipos, que por sus características técnicas y capacidades, son susceptibles de ser utilizados como equipos de emergencia del otro local, debiendo 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 recuperación de información posibiliten el funcionamiento adecuado de los sistemas.



Fuente: www.consultinginformationtechnology.com

CAPITULO IV

4.1 AUDITORIA AL PLAN DE CONTINGENCIA Y RECUPERACION ANTE DESASTRES

INTRODUCCION

La Auditoria informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes. En si la auditoria informática tiene 2 tipos las cuales son:

Auditoría Interna: es aquella que se hace adentro de la empresa; sin contratar a personas de afuera.

Auditoría Externa: como su nombre lo dice es aquella en la cual la empresa contrata a personas de afuera para que haga la auditoria en su empresa. Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Los objetivos de la auditoría son:

- El análisis de la eficiencia de los Sistemas de Información
- La verificación del cumplimiento de la Normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos.

Sus beneficios son:

- Mejora la imagen pública.
- Confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Disminuye los costos de la mala calidad (re-procesos, rechazos, reclamos, entre otros).
- Genera un balance de los riesgos en TI.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

*** Desempeño**

- Fiabilidad
- Eficacia
- Rentabilidad
- Seguridad
- Privacidad

Generalmente se puede desarrollar en alguna o combinación de las siguientes áreas:

*** Gobierno corporativo**

- Administración del Ciclo de vida de los sistemas
- Servicios de Entrega y Soporte
- Protección y Seguridad
- Planes de continuidad y Recuperación de desastres

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como Cobit, Coso e Itil, actualmente la certificación de ISACA para ser CISA *Certified Information Systems Auditor* es una de las más reconocidas y avaladas por los estándares internacionales

ya que el proceso de selección consta de un examen inicial bastante extenso y la necesidad de mantenerse actualizado acumulando horas (puntos) para no perder la certificación.

Tipos de Auditorias de Sistemas

- **Auditoría de los datos**: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
- **Auditoría de las bases de datos**: Controles de acceso, de actualización, de integridad y calidad de los datos.
- **Auditoría de la seguridad**: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- **Auditoría de la seguridad física**: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.
- **Auditoría de la seguridad lógica**: Comprende los métodos de autenticación de los sistemas de información.
- **Auditoría de las comunicaciones**. Se refiere a la auditoria de los procesos de autenticación en los sistemas de comunicación.
- **Auditoría de la seguridad en producción**: Frente a errores, accidentes y fraudes.

AUDITORIA MEDIANTE MODELO DE CHECKLIST

Cuando el Auditor SI, realiza una auditoria a los sistemas se apoya en diferentes tipos de herramientas para la evaluación de todos los componentes del sistema de información como por ejemplo confeccionar unos listados de chequeos, o modelos de Control, los cuales sirven para evaluar si las organizaciones están cumpliendo con las buenas prácticas establecidas para la seguridad de la información.

CHECK LIST:

CONOCIMIENTO DEL SISTEMA: *INVENTARIO*	SI	NO	N/A
La organización posee un inventario de los sistemas, hardware y datos			
El inventario ha sido revisado por un especialista externo (auditor, experto en informática...)			
Se sabe quienes son los dueños de los elementos que se encuentran en el inventario			
Se sabe quienes son los usuarios de los elementos del inventario			
Existe un criterio para definir cuales son los elementos críticos del inventario			
El criterio usado distingue entre: riesgos de la organización, a los ss. prestados a clientes y de interrupciones a los procesos de negocio			
El criterio ha sido validado por la administración de la organización y jefes de informática			
Se ha realizado un listado en forma descendente para determinar los elementos más críticos			
Las pruebas y actualizaciones se realizan de acuerdo al listado de prioridades			

CAPITULO V

RESULTADOS

5.1 CASO ENTIDADES PÚBLICAS

Caso 1. Municipalidad San Pedro de la Paz.

El 29 de Diciembre de 1995, el sector de San Pedro se convierte en comuna, pasando a llamarse San Pedro de la Paz, y estableciéndose su municipalidad en el barrio de la Villa San Pedro.

Reseña de la Comuna:

La historia de San Pedro de la Paz se remonta al1604, año en que el gobernador Alonso de Ribera, funda el **Fuerte de San Pedro**, con el fin de reforzar la línea defensiva que se estableció a lo largo del rio Bio Bio.

Entre 1877 y 1890, se construye un puente ferroviario sobre el rio Bio Bio, que permite la conexión de la zona carbonífera del sur de San Pedro de la Paz con el resto del país.

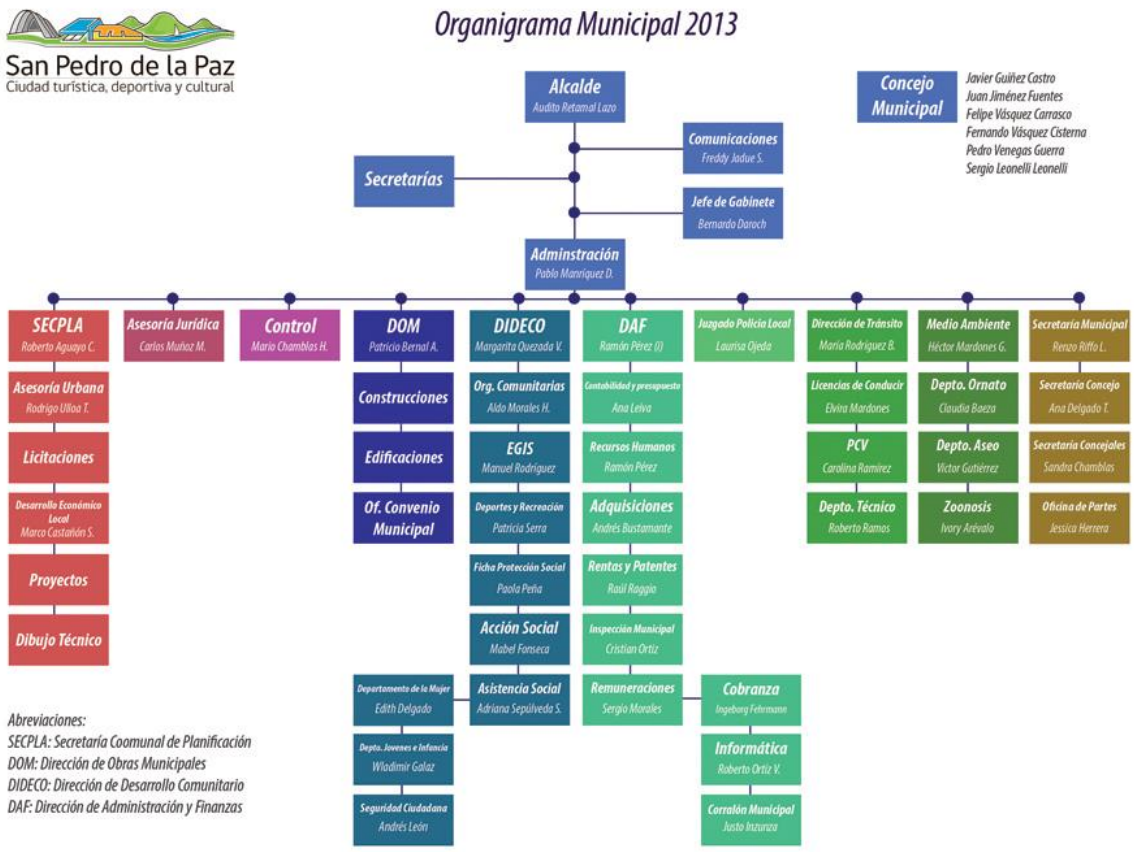
En mayo de 1943, se inaugura el primer puente carretero sobre el Biobío (Puente Biobío o Puente Viejo), con 1.648,5 metros de largo. Constituyó un hito importante para la comunidad, ya que permitió una conexión más expedita con Concepción.

El año 1974, todo el sector actualmente llamado San Pedro dependió de la comuna de Coronel, hasta que el régimen Militar crea la Provincia de Concepción y San Pedro pasa a depender del municipio Penquista hasta 1995.

San Pedro de la Paz está situada al sur y al poniente del rio Bio Bio, cercana al centro geográfico de Chile continental. La comuna tiene un clima templado, cálido y húmedo, tipo mediterráneo

Su actual Edil es el señor: Audito Retamal Lazo.

Organigrama Municipal



Encargado Área Informática, Municipalidad San Pedro de la Paz: Ricardo Tapia Almendra, Servicios contratados: sistemas de Adquisiciones, Bienes, Bienestar, Bodega, Contabilidad, Gestión documental, Juzgado policía local, licencias, Patentes municipales, Patenten Vehiculares, Personal, Reloj control, Tesorería y Remuneraciones.

Caso 2. Municipalidad de Chiguayante.

Reseña de la Comuna

El 07 de Octubre de 1925, por Decreto Presidencial, artículo 37, Nº 740, se crea por primera vez, la comuna de Chiguayante, siendo su primer alcalde don Walter Schaub, secretario don René Gárate y vocal don Jorge Wilson. Las sesiones eran el primer y tercer sábado de cada mes, ocupando como recinto municipal las dependencias de la familia Schaub.

Sin embargo, el 30 de Diciembre de 1927, nuevamente bajo Decreto presidencial se relega a Chiguayante a Subdelegación de Concepción (la comuna duró un año, 11 meses y 23 días). En 1990 vecinos y fuerzas vivas de Chiguayante crean el Comité Pro-comuna, el que estuvo representado por los señores Iván Francesconi, Hugo Moreno, Luis Peña y Sergio Albornoz, quienes abrigaban la esperanza de volver a independizar a esta localidad de Concepción. Luego, gracias al tesón y esfuerzo de este comité y del apoyo de los parlamentarios de la zona, el 28 de Junio de 1996, se publica en el Diario Oficial, la Ley Nº 19.461 que crea por segunda vez la comuna de Chiguayante.

El 27 de Octubre de ese mismo año la comunidad escoge a sus primeras autoridades, siendo electo alcalde, don Tomás Solís Nova y como concejales los señores Iván Francesconi, Jaime Bahamondes, Luis Stuardo, Osvaldo Gómez y Eleodoro Rivera, quienes asumieron en sus cargos, el 11 de Diciembre, ocupando las antiguas dependencias de la delegación.

Visión:

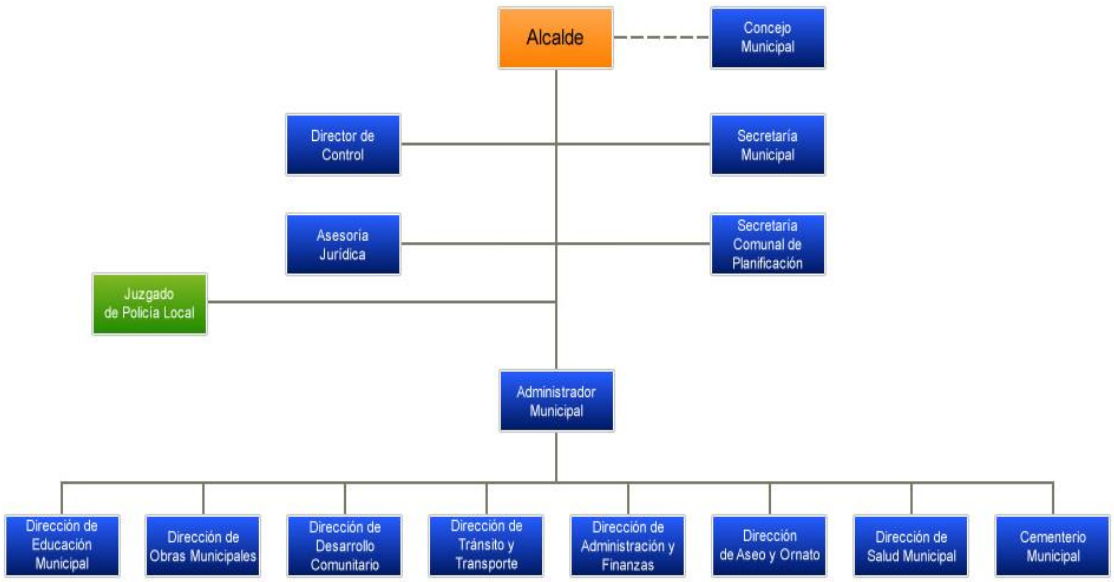
La Ilustre Municipalidad de Chiguayante se empeña en construir una Ciudad para vivir Residencial, Cultural, Fluvial, Turística, Productiva y Rentable.

Misión:

Construiremos una Ciudad para vivir, con el compromiso y esfuerzo de todos nuestros vecinos y proporcionándoles a ellos y los ciudadanos en general una atención de excelencia, con rapidez, eficiencia y amabilidad.

En la actualidad esta municipalidad de la Provincia de Concepción, se encuentra dirigida por el Edil, don José Antonio Rivas VillalobosLo mismo.

Organigrama Municipal



Encargado Área Informática, Municipalidad Chiguayante: Rubén Oses

Servicios contratados:

Sistemas de Adquisiciones, Bienestar, Bodega, Contabilidad, Gestión documental, Juzgado policía local, licencias, Patentes municipales, Patenten Vehiculares, Personal, Tesorería y Remuneraciones.

Juzgado policía local, licencias, Patentes municipales, Patenten Vehiculares, Personal, Reloj control, Tesorería y Remuneraciones

Caso 3. Municipalidad de Hualqui

Reseña de la Comuna

La Municipalidad de Hualqui se crea según el Diario Oficial el 22 de Diciembre de 1891, durante la República Parlamentaria (1891 - 1920), bajo el gobierno de Jorge Montt. El primer Alcalde fue Armando Méndez.

Cuando se fundó la municipalidad, los alcaldes eran elegidos por los regidores que eran cinco. Los regidores equivalen a los que hoy son los concejales. Los alcaldes duraban tres años, cuyo periodo se subdividía entre dos alcaldes, lo cual era acordado a través de pactos municipales.

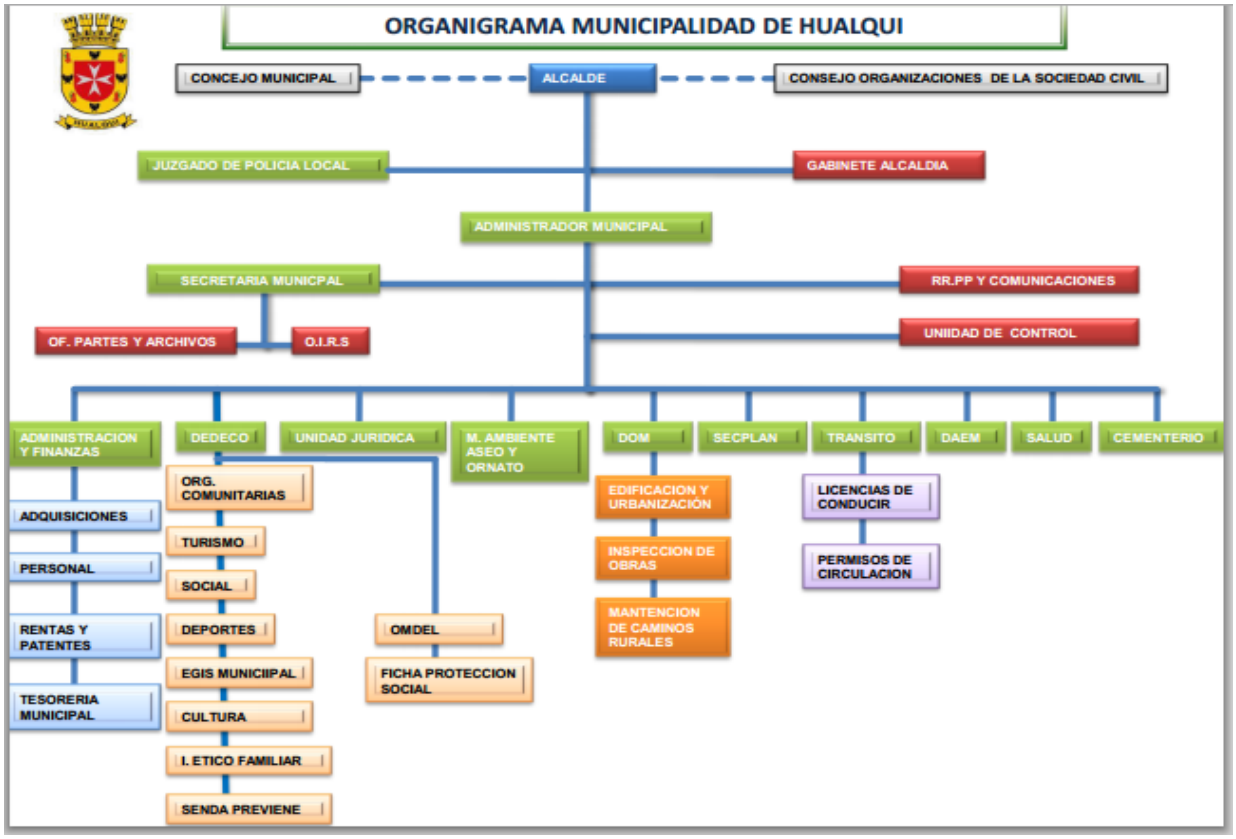
Hualqui con el devenir de los siglos se fue estableciendo como un pueblo, principalmente agrícola, que se caracteriza por su tranquilidad, privilegiado clima y la calidez y sencillez de su gente rural.

Hualqui fue fundada el 24 de octubre de 1757 por el Gobernador del reino de Chile don Manuel de Amat y Junient, ingresando a las páginas de la Historia con los Lavaderos de Oro de Pedro de Valdivia en Quilacoya.

Su historia comienza en 1552, específicamente, en el territorio que en la actualidad se conoce como Quilacoya. En aquel año el Gobernador don Pedro de Valdivia, descubrió ricos lavaderos de oro en la parte superior del río que baña aquel sector, estableciéndose un asiento de minas.

Edil actual Ricardo Fuentes Palma

5.3.2 Organigrama Municipal



Encargado Área Informática Municipalidad de Hualqui: Ronald Escalona Oñate.

Servicios contratados: sistemas de Adquisiciones, Contabilidad, Gestión documental, Juzgado policía local, licencias, Patentes municipales, Patenten Vehiculares, Personal, Tesorería y Remuneraciones.

Caso 4. SENDA Región del Bio Bio.

Reseña

Servicio Nacional para la Prevención y Rehabilitación del Consumo de Drogas y Alcohol (SENDA) es la entidad del Gobierno de Chile, responsable de elaborar las políticas de prevención del consumo de drogas y alcohol, así como de tratamiento, rehabilitación y reinserción social de las personas afectadas por estas sustancias.

El Servicio Nacional para la Prevención y Rehabilitación del Consumo de Drogas y Alcohol (SENDA), radicado en el Ministerio del Interior y Seguridad Publica, fue creado el 21 de febrero de 2011 por la ley Nro. 20.502.

Conforme a lo establecido en el Decreto con Fuerza Ley Nro. 2-20502, creó la planta funcionaria, inició oficialmente sus funciones el **1 de octubre de 2011**.

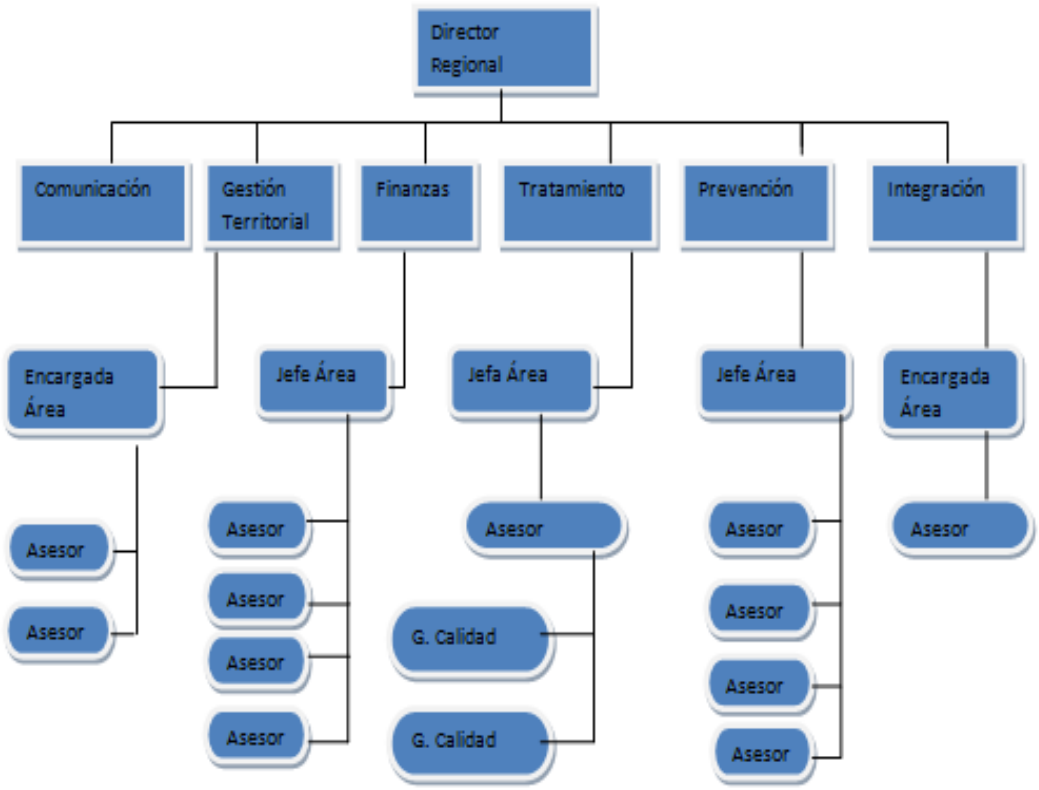
Por ley, este organismo tiene como misión:

- La ejecución de las políticas en materia de **prevención del consumo de estupefacientes**, sustancias psicotrópicas e ingesta abusiva de alcohol,
- La ejecución de políticas en materia de **tratamiento, rehabilitación y reinserción social** de las personas afectadas por dichos estupefacientes y sustancias psicotrópicas.
- La elaboración de una **estrategia nacional de drogas y alcohol (*)**

- Administrar el fondo establecido por el artículo 46 de la ley Nro. 20.000.
- SENDA dará continuidad a las labores que cumplía el Consejo Nacional para el Control de Estupefacientes (CONACE), creado mediante el Decreto Nro. 683 del 21 de Septiembre de 1990.
- Director regional: Byron Martínez Ulloa.
- Centros de tratamiento 17
- Senda Previene 31

Oficina regional ubicada en calle Tucapel 194 concepción.

5.4.2 Organigrama Senda Regional



Fuente: Senda Regional

En esta entidad Regional no existe un encargado del área TI. O persona con los conocimientos necesarios para la solución de alguna contingencia ya sea de Software o hardware.

Tampoco existen contratos con empresas externas, de servicios de TI, y estos son otorgados formalmente de Senda Nacional con ubicación en la Ciudad de Santiago desde donde otorgan los servicios de .tecnología mediante un sistema de gestión documental (SIDOC) un sistema de soporte técnico computacional (SISTCOM), y cuanto a los sistemas críticos financieros son soportados por el sistema de información para la gestión financiera (SIGFE), mediante servidor remoto, como medida o resguardo de la información, cada funcionario utiliza

medios propios, ya que no toda la información es ingresada a estos sistemas de gestión documental.

5.2 DIAGNOSTICO ENTIDADES PÚBLICAS

Este Capitulo presenta los resultados obtenidos de los Check List, aplicados a cuatro Servicios Públicos de la Región del Biobío. En función de los objetivos propuestos en la presente investigación. Los resultados se describen de acuerdo a:

1.- Conocimiento del Plan de Contingencia.

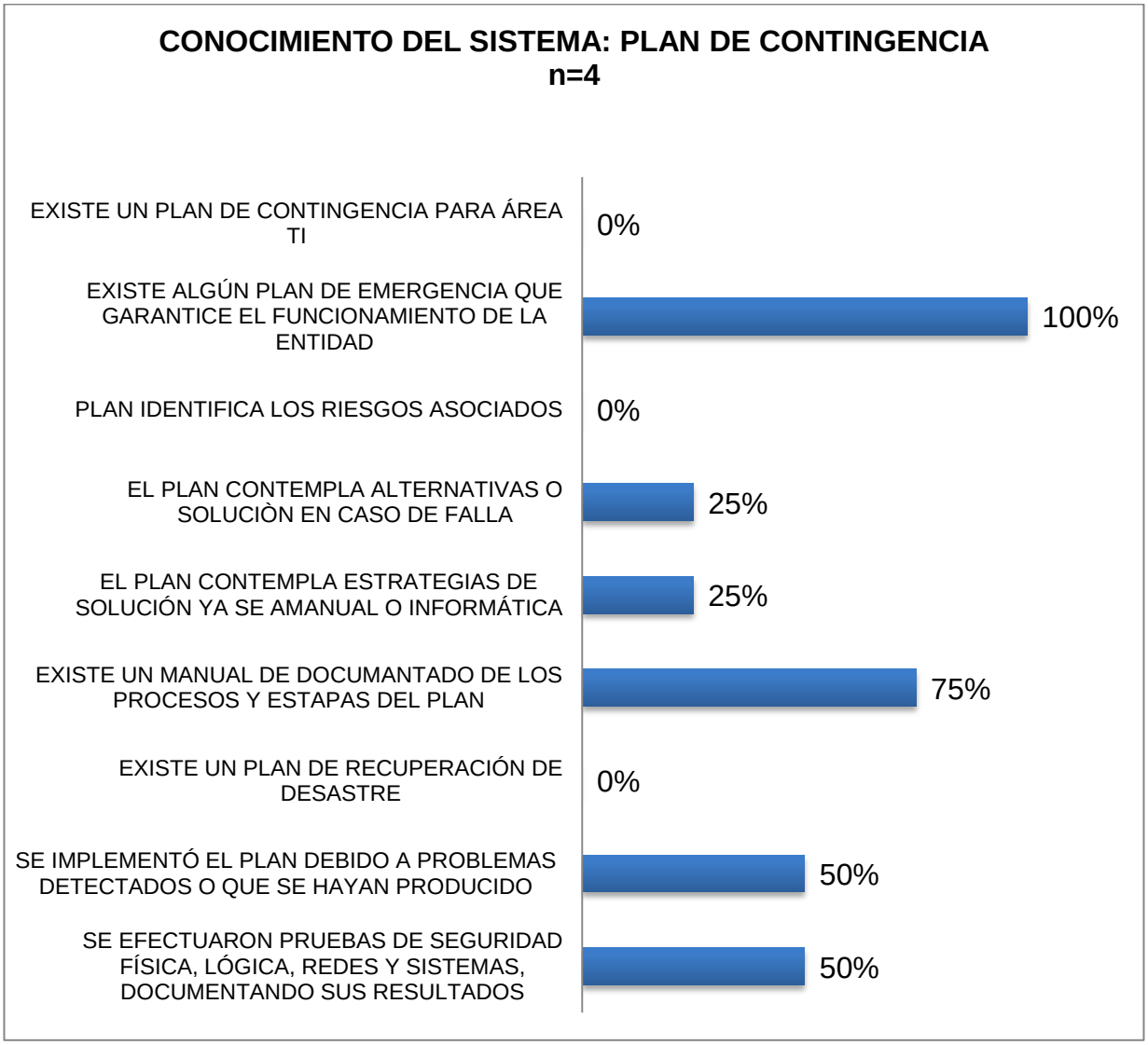
2.- Conocimiento de Inventario.

3.- Conocimiento en Seguridad Física, Lógica, Redes y Sistemas de conformidad a Normas y Estándares

4.- Evaluación riesgos por entidad.

1. **Conocimiento Plan de Contingencia**

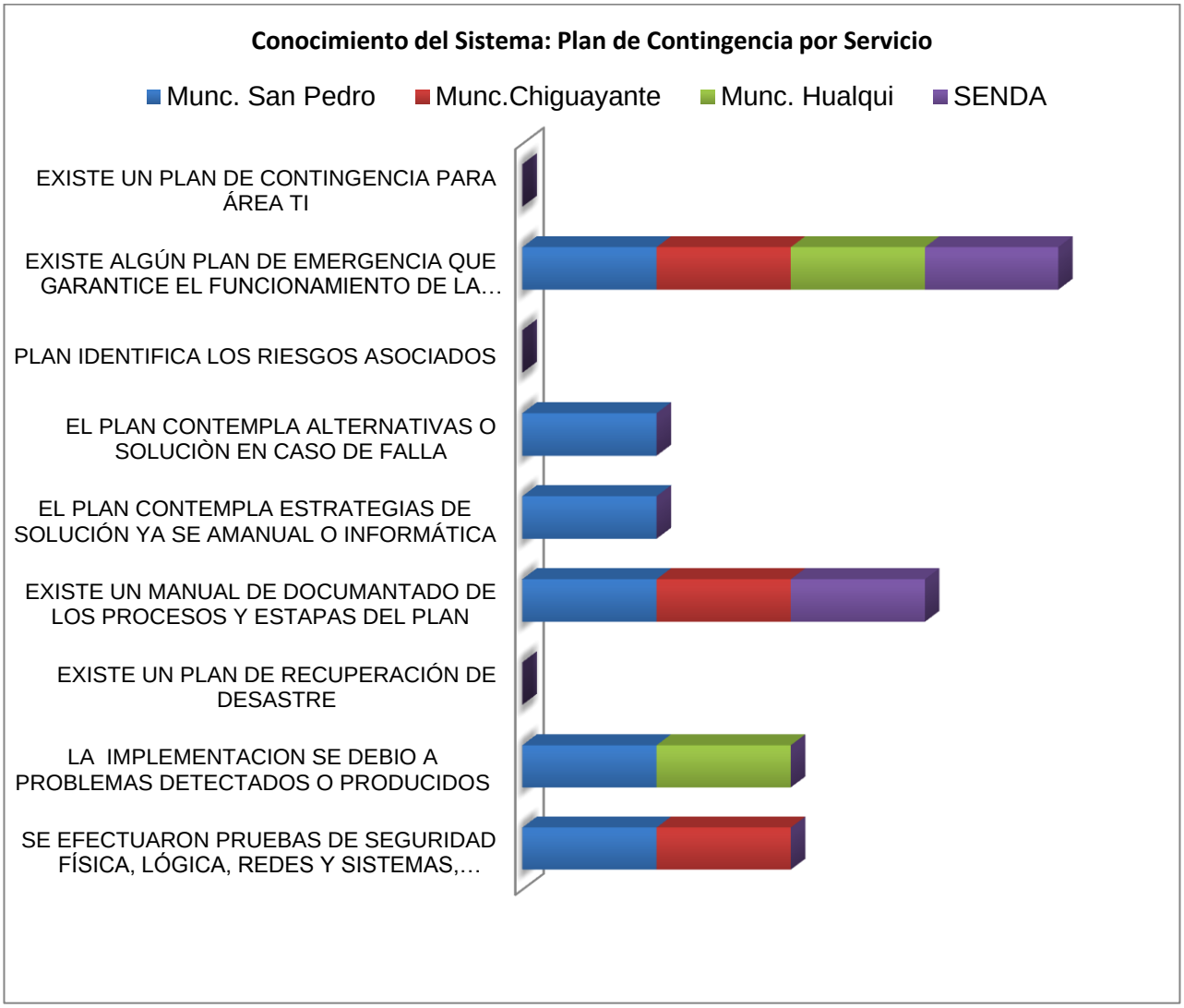
Toda entidad ya sea privada o pública debe contar con un plan de emergencia orientado a suplir las contingencias que debido a causas voluntarias o involuntarias puedan perjudicar el normal funcionamiento de la organización, por ende el conocimiento del plan por parte del encargado del área y aéreas en general asociadas a los procesos dependientes de las tecnologías de información y comunicación es primordial, los siguientes gráficos muestran el conocimiento por parte de los encargados del área Ti, del plan de contingencia.



Fuente: Check List aplicada a Entidades Públicas, Concepción 2015.

En relación al Conocimiento del Plan de contingencia en los Servicios Públicos Encuestado**, y** como muestra la Figura 1, el 100% de las entidades, no poseen un Plan de Contingencia, sin embargo el 100% posee otro Plan de Emergencia u otro que garantiza el funcionamiento del servicio, este plan no identifica todos los riesgos asociados, solo un 25% contempla alternativas en caso de fallas, un 25% contempla estrategias de solución, y el 75% posee un manual documentado de los procesos, se advierte además que ninguna entidad posee un Plan de recuperación ante desastres, solo un 50% señala haber implantado el plan debido a problemas detectados, y un 50% efectuó pruebas a la seguridad.

Figura 2: Conocimiento de Plan de Contingencia.



Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

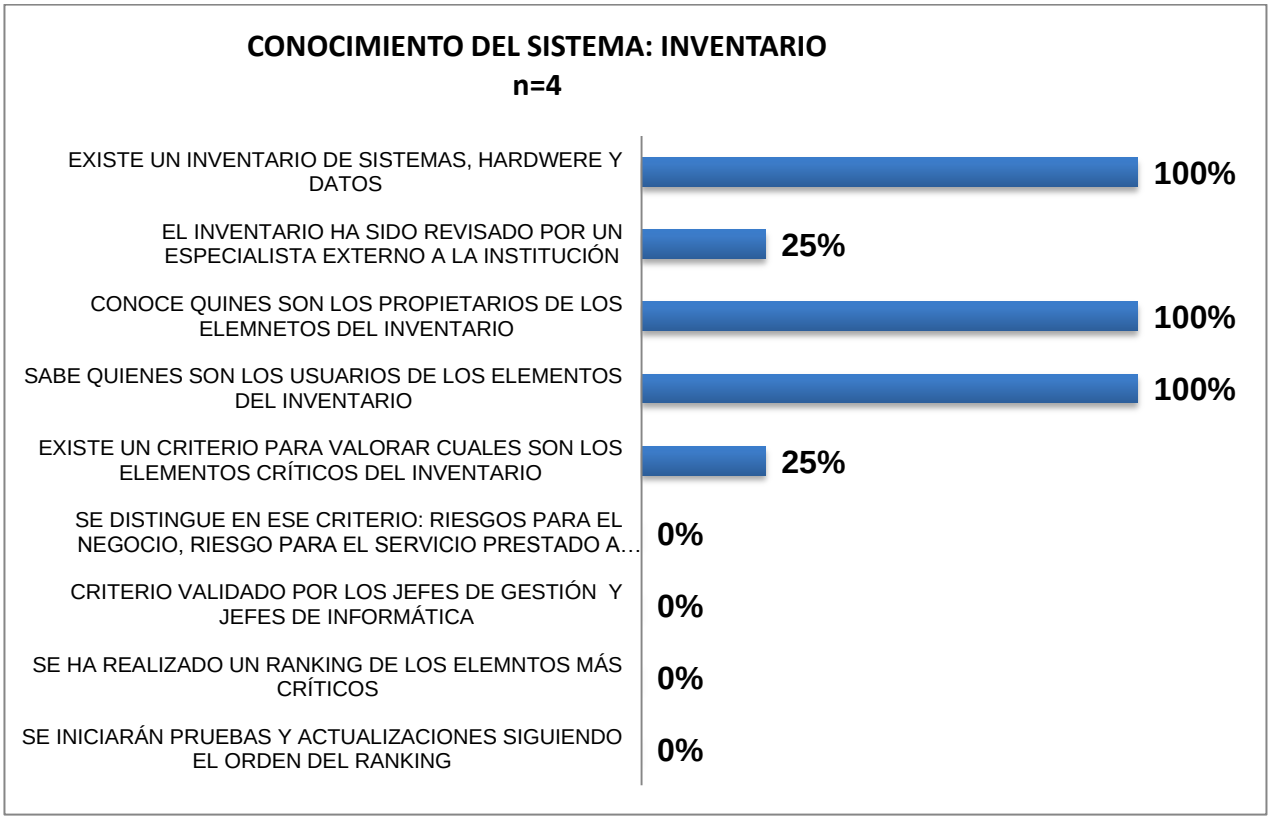
Del Mayor Conocimiento del Plan de Contingencia, cada rectángulo de color representa un 25%, respectivamente de los Servicios Públicos Encuestados, como muestra la figura 2, muestra que el 100% de las entidades no poseen un plan de contingencia, plan que identifica los riesgos asociados y tampoco un plan de recuperación ante desastres del área TI. Además

un 75 % no cumple con los criterios sobre el cumplimiento de alternativas o estrategias en caso de fallas

2. Conocimiento Sistema de Inventario

En base al Conocimiento de inventario de los sistemas que componen el área Ti, de la entidad podemos saber los riesgos asociados a ellos, ejemplarizando, (un equipo destinado al área Contable), posee mayor capacidad, mejores software y diferentes tipos de asignaciones con restricciones de usuarios, debido al tipo de información y su riesgo para el funcionamiento de la entidad, a diferencia del equipo de portería, por ende el conocimiento del inventario, sus usuarios y responsabilidades es de mucha importancia, los siguientes gráficos muestran el conocimiento del sistema de inventario en las entidades y por entidad.

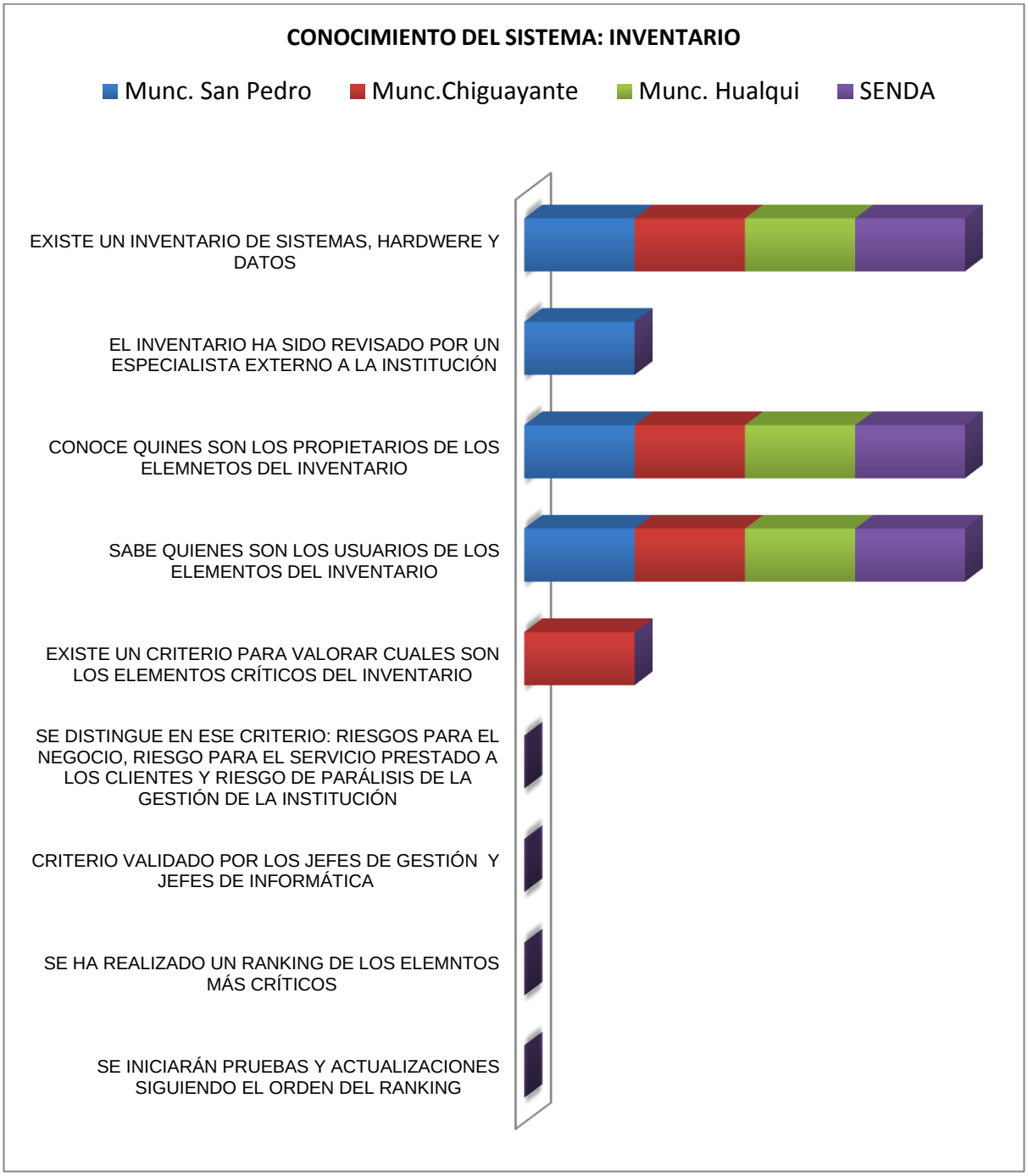
Figura 3: Conocimiento del Sistema Inventario.



Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

En relación al Conocimiento del Sistema Inventario, el 100% no conoce ni cumple con los criterios de valoración de los elementos críticos, no se distinguen los riesgos para el negocio y servicio no realizan un ranking de elementos críticos ni tampoco aplican pruebas mediante el ranking.

Figura 4: Conocimiento del Sistema Inventarios.



Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

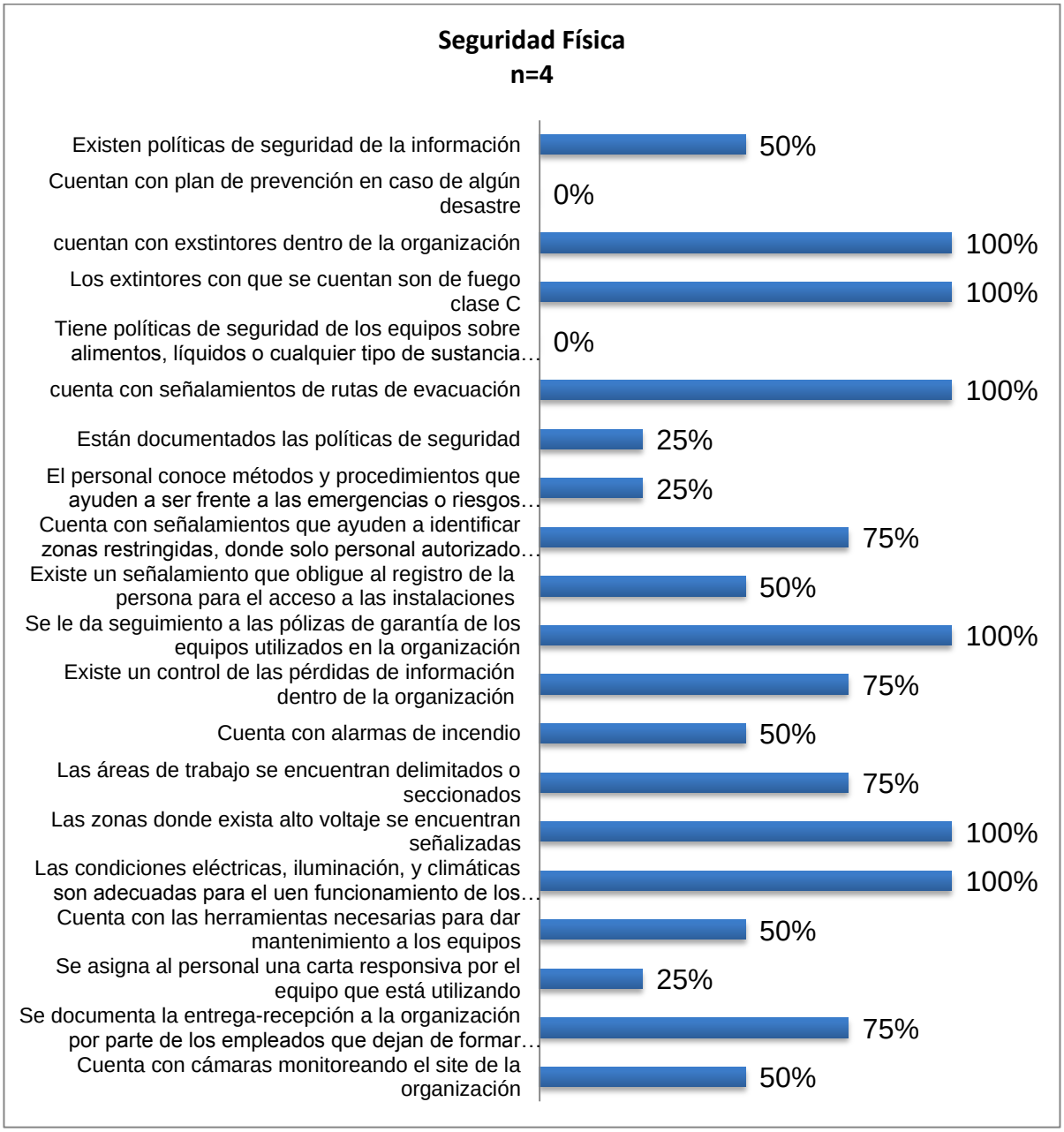
En relación al Conocimiento del Sistema Inventario, en los Servicios Públicos Encuestado, como muestra la figura 3, en las entidades el 100% de ellas existe: un inventario de sistemas Hardware y datos, conoce quienes son los propietarios de los elementos del inventario, y tiene conocimiento de los usuarios de cada elemento, solo un 25% utiliza algún criterio para evaluar los elementos críticos, del inventario, se sabe además que el 100% de ellas no cumple con distinguir los riesgos para el negocio, validar el criterio por los jefes de gestión e informática, poseer un ranquin de los elementos críticos, y por último las pruebas que se realizan no se efectúan mediante ningún ranking.

3. Conocimiento Seguridad Física

El conocimiento de la Seguridad Física, es primordial en la categorización del nivel de riesgos asociados no solo a los componentes físicos si no también a los riesgos propios de la entidad.

Esta seguridad garantiza la integridad de los activos humanos, lógicos y material de un Centro de Procesamiento de Datos.

Figura 5: Del cumplimiento de criterios de Seguridad Física en base a estándares.

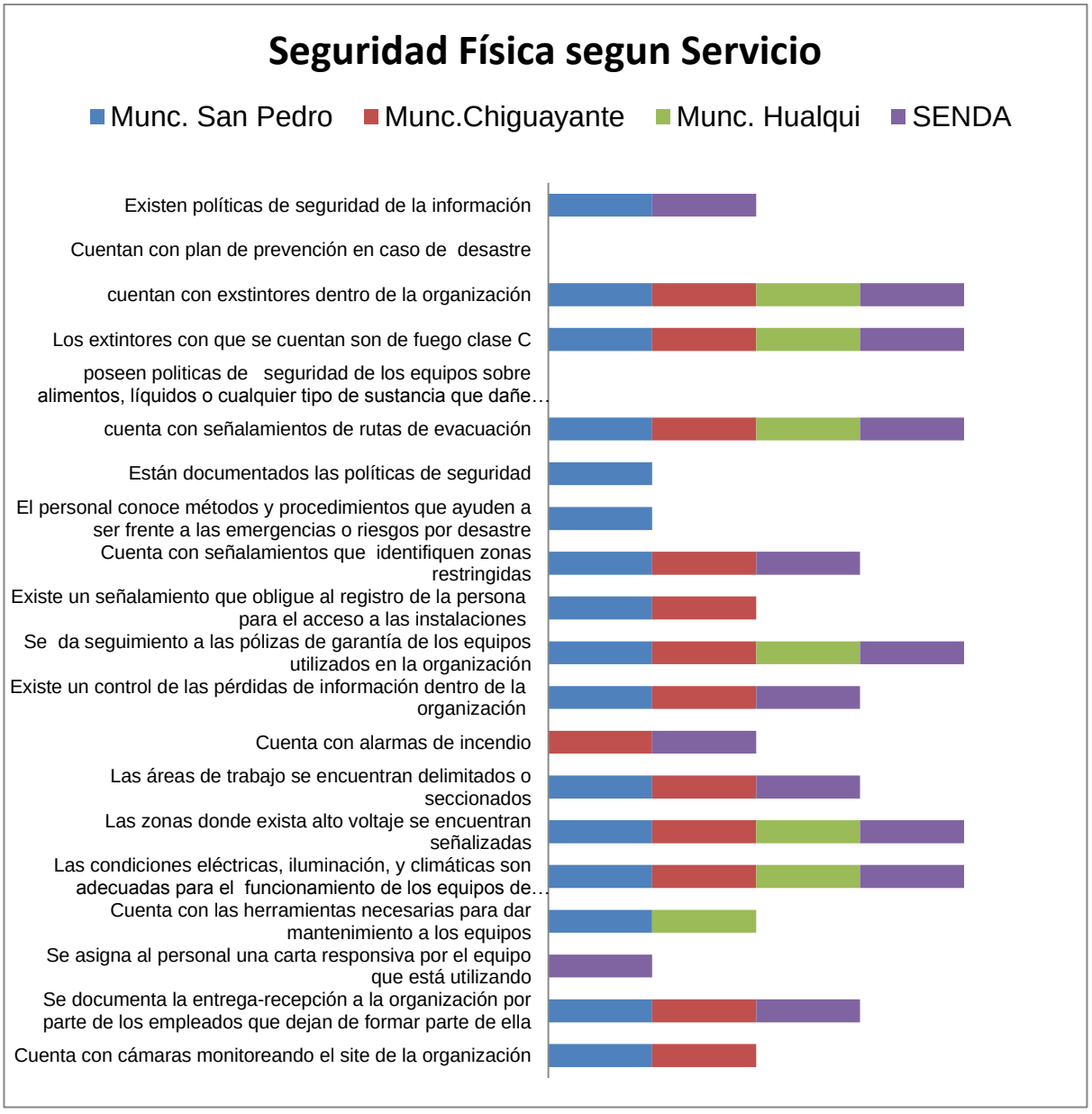


Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

En relación al cumplimiento de criterios de Seguridad Física, en base a estándares y normas, en los Servicios Públicos Encuestado, muestra que el 100 % de las entidades no cuentan con un plan en caso de desastres, tampoco cumple con políticas de seguridad respecto a líquidos

o sustancias que dañen los equipos, además un 75% no tiene documentada las políticas de seguridad, como tampoco su personal conoce métodos y procedimiento frente a desastres cumplimiento de estándares por entidad.

Figura 6, Entidad con mayor grado de seguridad física.



Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

Del Mayor Conocimiento y grado de Seguridad Física en los Servicios Públicos Encuestado, como muestra la figura 6, el Municipio de San Pedro de la Paz, posee un mayor conocimiento y aspectos de seguridad.

4. Conocimiento Seguridad Lógica

Al igual que en la seguridad física, la seguridad lógica es indispensable para el desempeño de la entidad y su continuidad.

Figura 7,Del cumplimiento de criterios de Seguridad Lógica

Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

El grafico nos muestra que el 100 % de las entidades no obliga al cambio de contraseñas un 75 % de ella no posee un estándar para las contraseñas, ni tampoco utilizan letras, símbolos y números para su creación, además solo un 50 % no cuenta con licencias de software, ni tampoco poseen un proceso para adquirirlas

Figura 8, Del cumplimiento de criterios de Seguridad Lógica en base a estándares

Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

La figura nos muestra que las entidades solo cumplen 6 estándares y normas en un 100%, de un total 21 de seguridad lógica.

5. Conocimiento Seguridad en Redes

La seguridad involucra las instalaciones de las redes que alimentan, almacenan y brindan seguridad a los usuarios, de los sistemas y sus accesos.

Figura 9. Del cumplimiento de criterios de Seguridad en redes según estándares

Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

El grafico muestra que el100 % de las entidades no se apega a ningún estándar para asignar el cableado eléctrico, que un 75% de ellas tampoco cuenta con reguladores de energía por PC, ni con sistemas de protección de descargas electromagnéticas, que el 50% no cumple con estándares de tierra física según requisito establecido en las normas.

Figura 10, Seguridad en redes

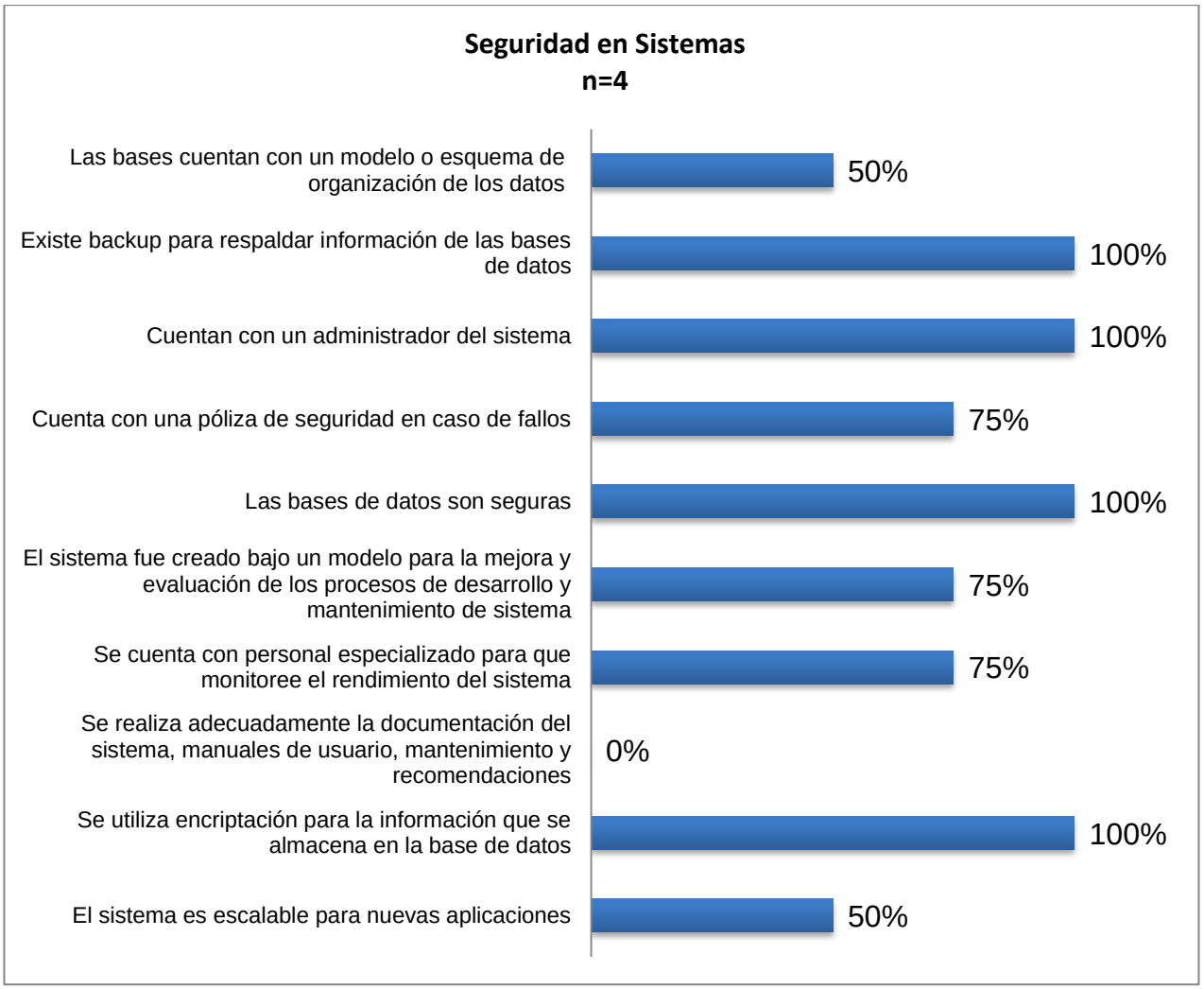
Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

El grafico nos muestra la entidad con mayor grado y/o conocimiento en seguridad en redes, además que el 100% de ellas se apega a algún estándar para asignar el cableado eléctrico.

6. Conocimiento Seguridad Sistemas

El conocimiento en seguridad de sistemas apoya a la seguridad de todos los componentes, de la información critica, su resguardo, administración y respaldo.

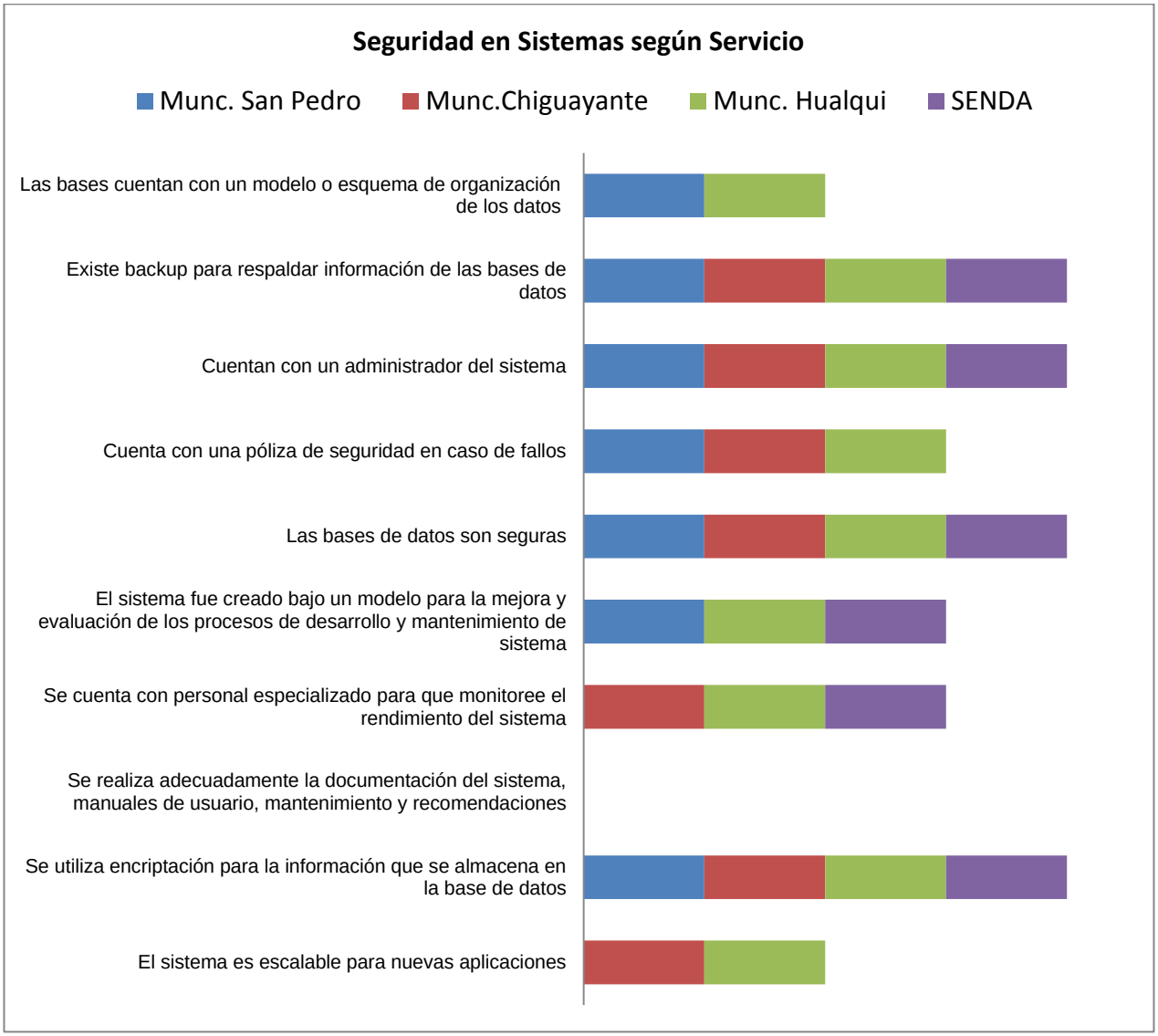
Figura 11. Del cumplimiento de criterios de seguridad en sistemas



Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

El grafico nos muestra que el 100% de las entidades no realiza la documentación del sistema, manuales de usuario o mantenimiento y recomendaciones, que el 50% de ellas, sus bases no cuentan con un modelo o esquema de organización de datos. Y su sistema no es escalable para nuevas aplicaciones.

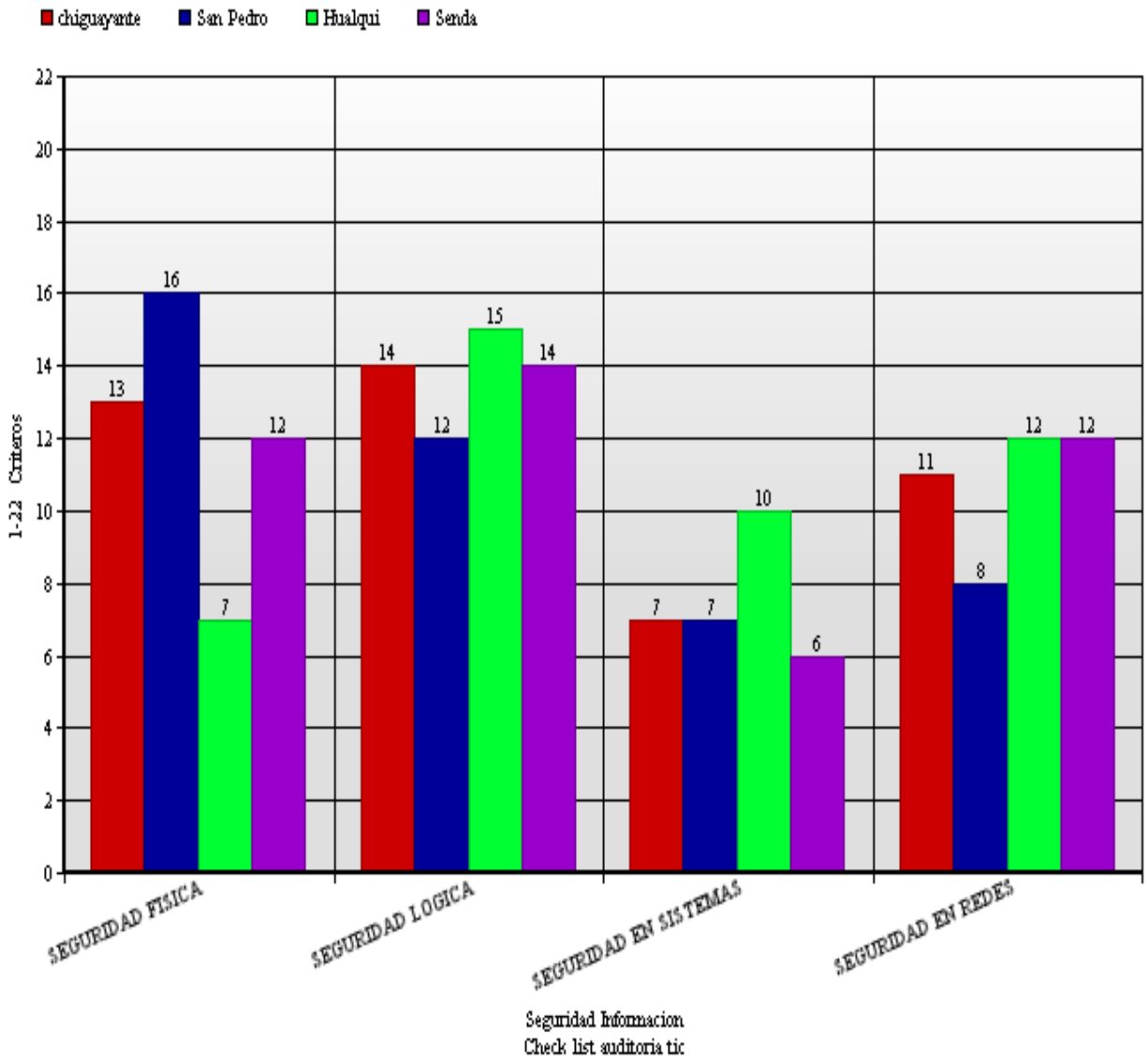
Figura 12, Seguridad de sistemas mediante estándares, Cada rectángulo tiene un valor especifico de un 25%



Fuente: Check List aplicada a Entidades Públicas, Concepción 2015

El grafico nos muestra la entidad con mayor cumplimento de criterios de seguridad de sistemas, siendo cada rectángulo un 25 %, mostrando a la Municipalidad de Hualqui quien cumple con una mayor cantidad de criterios de seguridad en sistemas también muestra que el 100% de las entidades no realiza adecuadamente la documentación del sistema, manuales de usuario, mantenimiento y recomendaciones totalidad de las entidades.

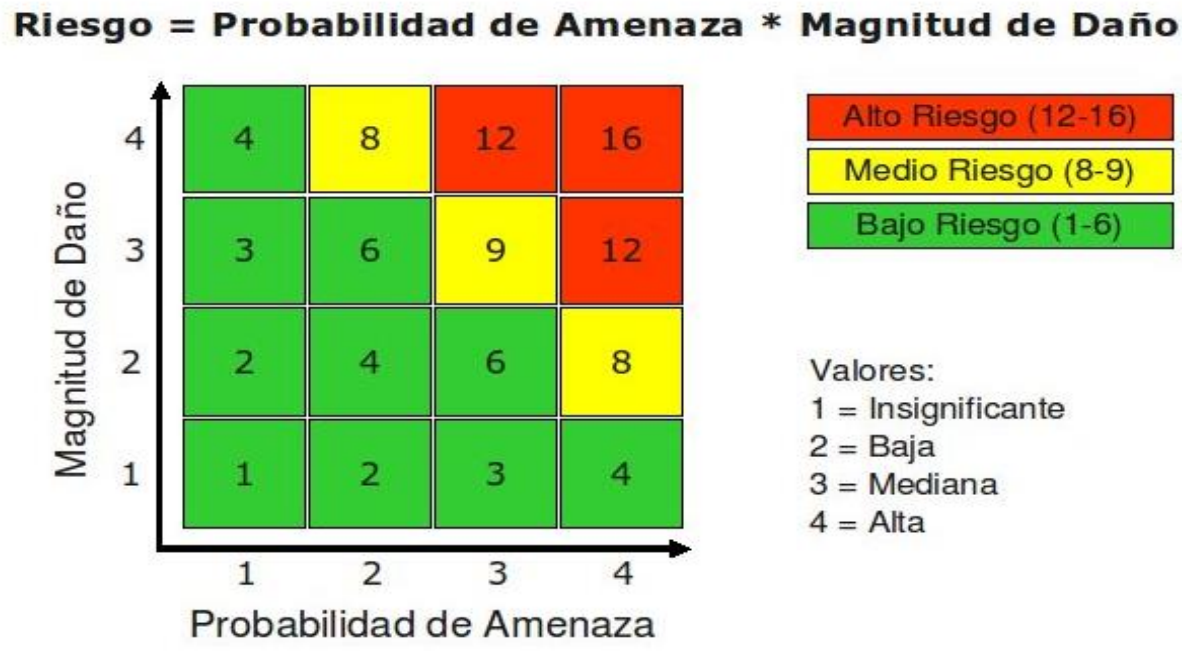
Figura 13. Del mayor grado de criterios de seguridad cumplido por entidad



San Pedro de la paz cumple con 43 criterios de un total de 80, siendo solo un 53.7%, Chiguayante cumple con 45 criterios de 80, siendo un 56.2%, Hualqui cumple con 44 criterios de 80 equivalente a un 55% y Senda cumple con 44 de un total de 80 criterios que representa también el 55%, mostrando todo esto, una falencia en la seguridad de los componentes Ti y riesgo para la entidad y sus procesos.

3. Evaluación de Riesgos Asociados a las Entidades Encuestadas

Con el objeto de entender mejor los resultados obtenidos se presenta a continuación una imagen de una matriz de riesgo.



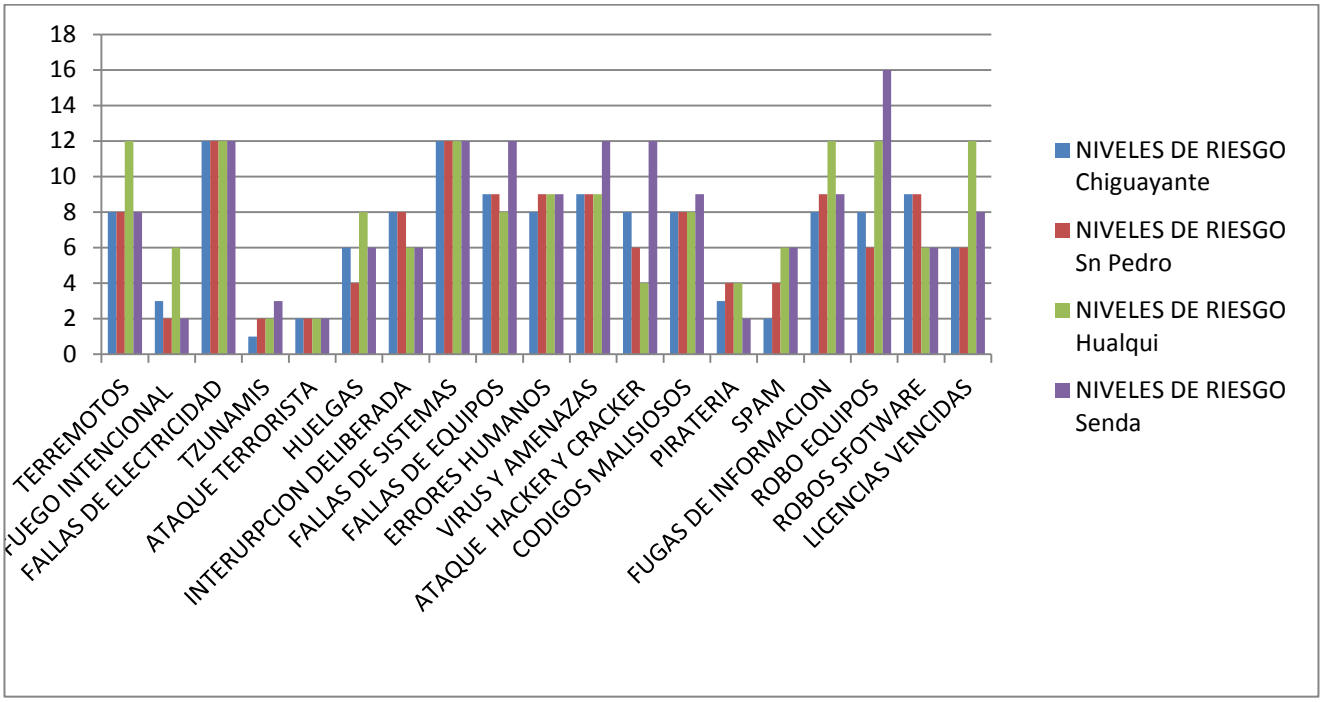
Fuente: www.protegete.wordpress.com

TABLA DE RIESGOS POR ENTIDADES ENCUESTADAS

TIPO DE RIESGO	PROBABLIDAD DE OCURENCIA				IMPÁCTO O MAGNITUD				NIVELES DE RIESGO POR ENTIDAD			
	C	S.P	H	S	C	S.P	H	S	Chigte	Sn Pedro	Hualqui	Senda
TERREMOTOS	2	2	3	2	4	4	4	4	8	8	12	8
FUEGO INTENCIONAL	1	1	2	1	3	2	3	2	3	2	6	2
FALLAS DE ELECTRICIDAD	4	3	4	4	3	4	3	3	12	12	12	12
TZUNAMIS	1	1	1	1	1	2	2	3	1	2	2	3
ATAQUE TERRORISTA	1	1	1	1	2	2	2	2	2	2	2	2
HUELGAS	2	2	2	2	3	2	4	3	6	4	8	6
INTERURPCION DELIBERADA	2	2	2	2	4	4	3	3	8	8	6	6
FALLAS DE SISTEMAS	4	4	3	3	3	3	4	4	12	12	12	12
FALLAS DE EQUIPOS	3	4	4	4	3	3	2	3	9	9	8	12
ERRORES HUMANOS	2	3	3	3	4	3	3	3	8	9	9	9
VIRUS Y AMENAZAS	3	3	3	4	3	3	3	3	9	9	9	12
ATAQUE HACKER Y CRACKER	2	2	2	3	4	3	2	4	8	6	4	12
CODIGOS MALISIOSOS	2	2	2	3	4	4	4	3	8	8	8	9
PIRATERIA	1	2	2	1	3	2	2	2	3	4	4	2
SPAM	2	2	3	3	1	2	2	2	2	4	6	6
FUGAS DE INFORMACION	2	3	4	3	4	3	3	3	8	9	12	9
ROBO EQUIPOS	2	2	3	4	4	3	4	4	8	6	12	16
ROBOS SFOTWARE	3	3	2	2	3	3	3	3	9	9	6	6
LICENCIAS VENCIDAS	2	3	4	2	3	2	3	4	6	6	12	8

Fuente: elaboración propia

TIPO DE RIESGO	NIVELES DE RIESGO POR ENTIDAD			
	Chiguayante	Sn Pedro	Hualqui	SENDA
TERREMOTOS	8	8	12	8
FUEGO INTENCIONAL	3	2	6	2
FALLAS DE ELECTRICIDAD	12	12	12	12
TZUNAMIS	1	2	2	3
ATAQUE TERRORISTA	2	2	2	2
HUELGAS	6	4	8	6
INTERURPCION DELIBERADA	8	8	6	6
FALLAS DE SISTEMAS	12	12	12	12
FALLAS DE EQUIPOS	9	9	8	12
ERRORES HUMANOS	8	9	9	9
VIRUS Y AMENAZAS	9	9	9	12
ATAQUE HACKER Y CRACKER	8	6	4	12
CODIGOS MALISIOSOS	8	8	8	9
PIRATERIA	3	4	4	2
SPAM	2	4	6	6
FUGAS DE INFORMACION	8	9	12	9
ROBO EQUIPOS	8	6	12	16
ROBOS SFOTWARE	9	9	6	6
LICENCIAS VENCIDAS	6	6	12	8



El presente grafico muestra los niveles de riesgo por entidad de conformidad a los riesgos mencionados en la tabla anterior

5.3 PROPUESTA PLAN DE RECUPERACION ANTE DESASTRE MEDIANTE UN PLAN DE CONTINGENCIA TI.

La elección y adopción del modelo para un plan de contingencia y recuperación ante desastres fue evaluada mediante a los principales problemas que presentan las entidades como la falta de planes de contingencia y recuperación ante desastres, una inadecuada evaluación de riesgos, desconocimiento en seguridad ya sea física, lógica, redes y sistemas.

1. PLANIFICACIÓN

1-1 Diagnóstico

Es necesario siempre la revisión exhaustiva de cada uno de los componentes que conforman nuestro sistema, por ello, debemos realizar una etapa de diagnostico para poder asegurar que las acciones de solución propuestas tengan un fundamento realista y no tener que volver a rehacer toda propuesta.

Dentro del diagnostico se deben considerar cuatro factores que son:

- **Organización funcional y estructural:** se trata del organigrama el cual generalmente se detallan los departamentos que posee la organización, haciendo mención a cada una de las funciones que realiza cada departamento

- **Servicios y/o bienes producidos:** hace referencia a los servicios o bienes que produce la organización priorizando lo que genera más beneficios

- **Servicios y materiales utilizados:** hace mención a todos los servicios que son utilizados por la organización, como son electricidad, agua, transporte, materias

primas, insumos para la producción de información, todo esto debe ser detallado en una lista dando orden respecto a su significancia en los procesos de la organización.

- **Inventario de recursos informáticos:** Finalmente, se realiza un inventario detallando por departamento y en forma clasificada todos los activos de tecnologías de información que la organización posee. Entre estos activos se pueden encontrar programas, computadores, equipos empotrados, entre otros

El inventario de recursos informáticos se realizará por dependencias y en forma clasificada:

- Computadoras.
- Programas.
- Aplicativos Informáticos.
- Equipos Empotrados

.

El procesamiento de este inventario puede ser de dos tipos:

- **Proceso Automatizado**.- Utilizando herramientas informáticas de diferente nivel, grado de detalle y costo, que pueden acelerar el tiempo de la toma del inventario, procesamiento de datos y emisión de resultados.
- **Proceso Manual**.- Utilizando formatos de recopilación de información.

El conocimiento del Inventario de estos recursos nos permitirá hacer una Evaluación de los Riesgos de la operatividad de los sistemas de información. Cada formato consta de dos partes:

a.- Datos componentes: Donde se registran los datos básicos de ubicación, identificación y características primarias, así como también su importancia, compatibilidad y adaptabilidad.

b.- Análisis del proceso de adaptación del componente:

Incluye datos de costos, fecha de culminación, medios utilizados y medidas de contingencia.

La fase de planificación es la etapa donde se define y prepara el esfuerzo de planificación de contingencia/continuidad. Las actividades durante esta fase incluyen:

- Definición explícita del alcance, indicando qué es lo que se queda y lo que se elimina.
- Definición de las fases del plan
- Definición de una estrategia de planificación de la continuidad del negocio de alto nivel.
- Identificación y asignación de los grupos de trabajo iniciales. definición de los roles y responsabilidades.
- Definición de las partes más importantes de un cronograma maestro y su patrón principal.
- Identificación de las fuentes de financiamiento y revisión del impacto sobre los negocios.
- Enfoque y comunicación de las metas y objetivos, incluyendo los objetivos de la empresa.
- Definición de estrategias para la integración, consolidación, rendición de informes y arranque.
- Desarrollo de un plan de alto nivel, incluyendo los recursos asignados.

Seguridad Integral de la Información

El procesamiento de datos, apoya no sólo a los sistemas de información administrativa sino también a las operaciones funcionales.

Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren.

2. IDENTIFICACIÓN DE RIESGOS

Busca minimizar las fallas generadas por cualquier caso en contra del normal desempeño de los sistemas de información.

En primer lugar se debe realizar un análisis del impacto que causaría en la organización una falla e incidente en la plataforma tecnológica o un desastre natural.

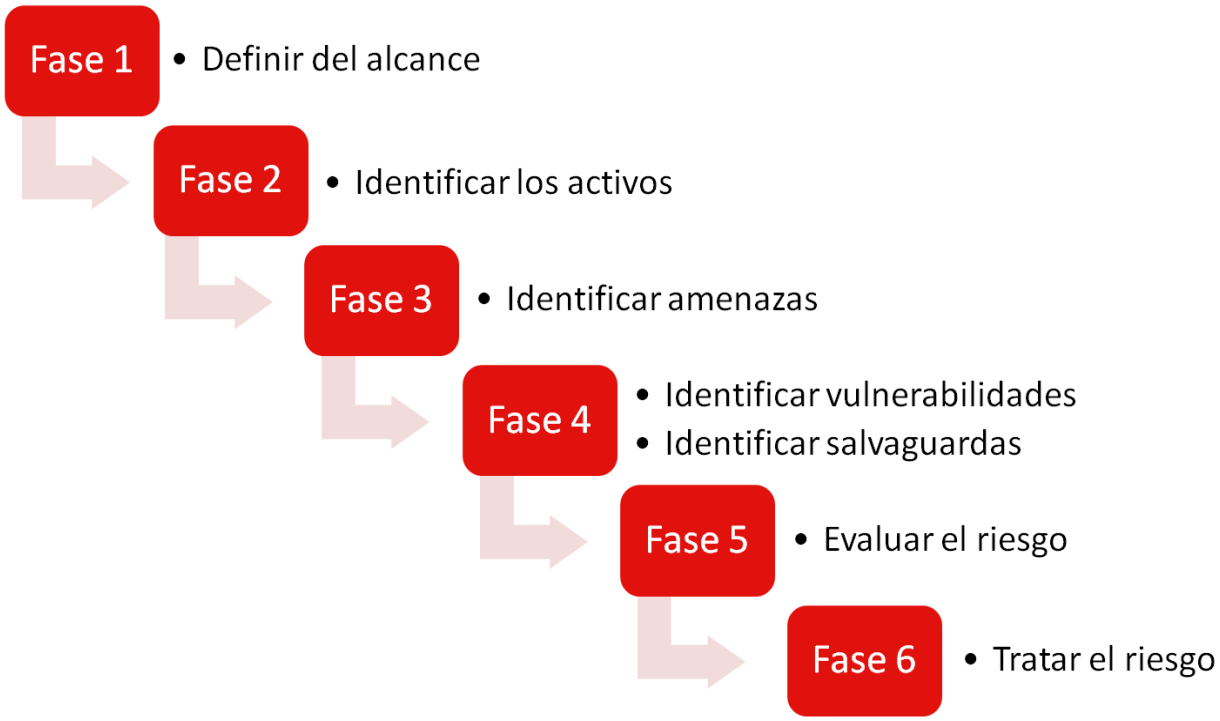
Se identifican los procesos críticos y consecuencias que se presentan en caso de no estar en funcionamiento, el primer componente del plan debe ser una descripción del servicio, también es recomendable determinar el costo que representa para la organización experimentar estos incidentes,

2.1 Análisis y Evaluación de Riesgos

El análisis del riesgo es uno de los trabajos más importantes a la hora de definir proyectos e iniciativas para la mejora de la seguridad de la información, considerando que las herramientas tecnológicas y la información son de gran valor para la organización.

En el caso que nos ocupa hemos seleccionado un conjunto de fases que son comunes en la mayor parte de las metodologías para el análisis del riesgo pero no menos efectivas.

Mediante fases:



Fuente:

https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/analisis_riesgos_pasos_sencillo

Fase 1. Definir el alcance

El primer paso del análisis de riesgos es establecer el alcance del estudio.

Hasta donde vamos a llegar, cuanto vamos a analizar, si este se va a realizar por áreas, departamentos, procesos o sistemas

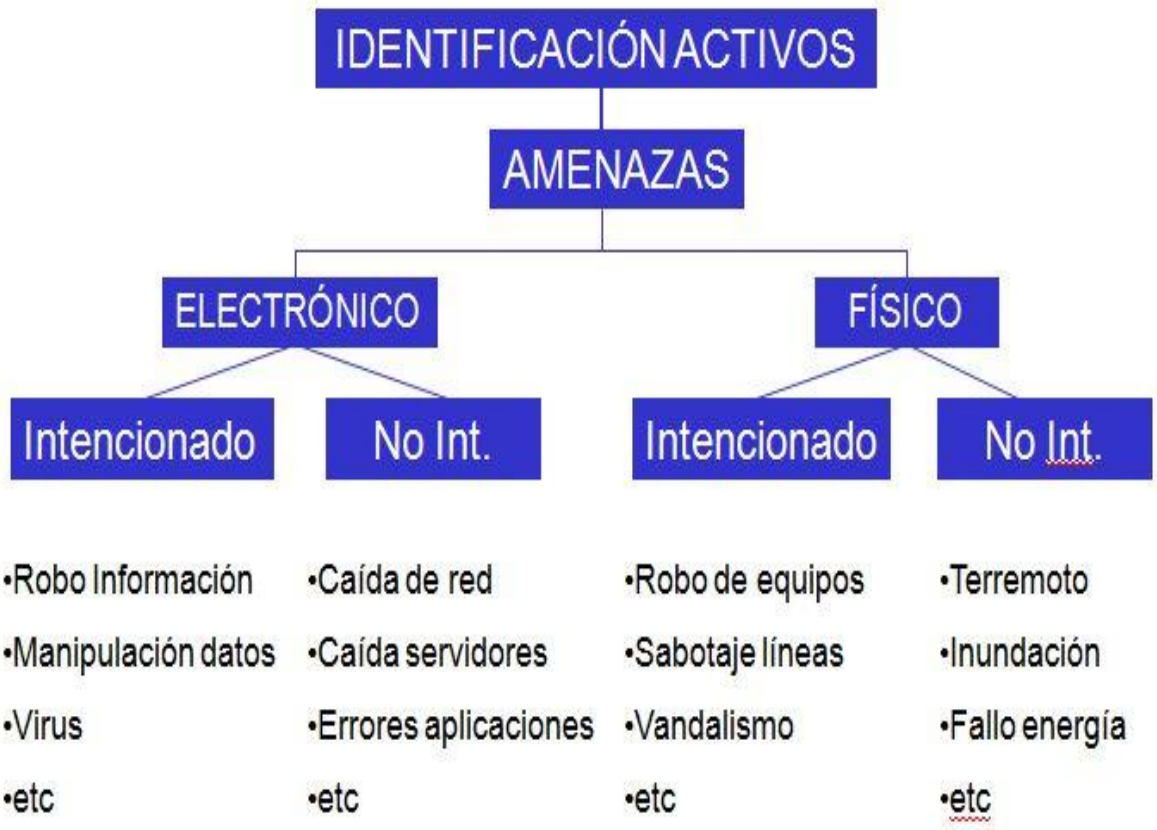
Fase 2. Identificar los activos

Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio.

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
...						

Fase 3. Identificar / seleccionar las amenazas

Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos.



Fuente: http://www.eoi.es/blogs/innovando/

Fase 4. Identificar vulnerabilidades y salvaguardas

La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades. Por ejemplo, un conjunto de ordenadores o servidores cuyos sistemas antivirus no están actualizados.

Fase 5. Evaluar el riesgo

Llegado a este punto disponemos de los siguientes elementos:

Inventario de activos.

Conjunto de amenazas a las que está expuesta cada activo.

Conjunto de vulnerabilidades asociadas a cada activo (si corresponde).

Conjunto de medidas de seguridad implantadas

Con esta información, nos encontramos en condiciones de calcular el riesgo.

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

Tabla para el cálculo del impacto

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Fuente:https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/analisis_riesgos_pasos_sencillo

Cálculo del riesgo

A la hora de calcular el riesgo, si hemos optado por hacer el análisis cuantitativo, calcularemos multiplicando los factores probabilidad e impacto:

RIESGO = PROBABILIDAD x IMPACTO.

Si por el contrario hemos optado por el análisis cualitativo, haremos uso de una matriz de riesgo como la que se muestra a continuación:

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Tal y como indicábamos en el apartado anterior, cuando vayamos a estimar la probabilidad y el impacto debemos tener en cuenta las vulnerabilidades y salvaguardas existentes. Por ejemplo, la caída del servidor principal podría tener un impacto alto para el negocio. Sin embargo, si existe una solución de alta disponibilidad (*Ej*. Servidores redundados), podemos considerar que el impacto será medio.

Fase 6. Tratar el riesgo

Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido .Por ejemplo, trataremos aquellos riesgos cuyo valor sea superior a "4" o superior a "Medio" en caso de que hayamos hecho el cálculo en términos cualitativos. A la hora de tratar el riesgo, existen cuatro estrategias principales:

Transferir el riesgo a un tercero. Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.

Eliminar el riesgo. Por ejemplo, eliminando un proceso o sistema que está sujeto a un riesgo elevado. En el caso práctico que hemos expuesto, podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.

2.2 Identificar los Procesos Críticos

Comenzar por los riesgos ya identificados como prioridades máximas porque causarían el mayor impacto negativo en los servicios y en las funciones críticas de su organización.

2.3 Análisis de las Operaciones Actuales

El análisis de operación del método actual de trabajo puede revelar las Oportunidades para reducir, eliminar o simplificar ciertas operaciones o procesos. Como son,

- Organización.
- Función. Funciones características serían ventas y mercadeo, contabilidad, ingeniería de desarrollo, compras y garantía de calidad.
- Proceso. actividad que emplea un insumo, le agregue valor y suministre el producto.
- Proceso de producción.
- Proceso de la empresa.

2.4 Uso de la Técnica de Análisis de Procesos

Analizando detalladamente los procesos podemos distinguir el siguiente flujo:

1. El ciclo de vida empieza con la descripción de un proceso basado en las metas del proyecto, mientras se utilizan los recursos descritos del proceso.
2. El proceso se fija al asignar los recursos.
3. El proceso puede instalarse en una máquina o pueden ser procedimientos a seguir por un grupo de personas.
4. El proceso es supervisado y medido durante su uso.
5. Los datos obtenidos de esta medida se evalúan durante todo el tiempo que se desenvuelva el proceso.

El Proceso de Dirección del Ciclo de Vida describe los componentes del proceso y la producción de los principales insumos de trabajo. La descripción del proceso funcionalmente se descompone en:

- Análisis del Proceso
- Plan del Proceso
- Aplicación del Proceso

3. IDENTIFICACIÓN DE SOLUCIONES

Un proyecto de plan de contingencia no sirve si se queda en plan o papel.

La magnitud, de un plan de contingencia será proporcional a la complejidad, importancia,

Costo del servicio al cual está destinado a proteger y el riesgo asociado a la misma.

El esquema general del plan de contingencias de los sistemas de información, esta

Constituido por 3 grandes fases:

- Fase de Reducción de Riesgos
- Fase de Recuperación de Contingencia
- Fase de Organización de un Sistema de Alerta contra Fallas

Matriz de planificación de contingencia y ejemplos

OPCIONES	OPERACIÓN MANUAL	REEMPLAZO	EXTERNALIZACION DEL SERVICIO
Reparación rápida y de defecto	Recurra al proceso manual sólo en caso de clientes prioritarios. Asegure que contará con personal el 1 y 2 de enero.	Tenga disponible software de repuesto que cumpla con los requisitos	Use personal temporalmente para llenar brecha
Reparación parcial	Use hojas de cálculo o base de datos para ofrecer alguna de la funcionalidad original del sistema (fecha de captura).	Use base de datos o paquetes COTS para reemplazar la funcionalidad del sistema	Haga que el contratista procese los pagos en sus propias instalaciones
Reparación total	Ofrezca operaciones totalmente funcionales a través del proceso manual, utilizando personal adicional si es necesario	Elimine esfuerzos de reparación e implemente un sistema comercial funcional, rápidamente	Entregue el manejo de la plantilla de pago a una firma comercial especialista

3.1 Identificación de Alternativas

La identificación de alternativas consiste en revisar los planes de administración de emergencia o recuperación de fallas. Estos son algunos ejemplos de alternativas que pudieran ayudarle al inicio del proceso de preparación.

- Planifique la necesidad de personal adicional para atender los problemas que ocurran.
- Recurra al procesamiento manual (de facturas, órdenes, cheques, etc.) si fallan los sistemas automatizados.
- Planifique el cierre y reinicio progresivo de los dispositivos y sistemas que se consideran en riesgo.
- Instale generadores si no tiene acceso a la red de energía pública.
- Disponga del suministro adicional de combustible para los generadores, en caso de fallas eléctricas prolongadas.
- Disponga de bombas manuales de combustible y úselas si fallan las electrónicas.
- Elaborar un programa de vacaciones que garantice la presencia permanente del personal.
- No haga nada y vea qué pasa – esta estrategia es algunas veces llamada arreglar Sobre falla.

3.2 Identificación de Eventos Activadores

los activadores provocarán la implementación del plan. Los activadores son aquellos eventos que permitirán decir “OK”, es el momento de pasar al plan B”.

A continuación se muestran algunos ejemplos de los tipos de eventos que pueden servir como activadores en sus planes de contingencia:

- Información de un vendedor respecto a la tardía entrega o no disponibilidad de un componente de software.
- Tardío descubrimiento de serios problemas con una interfaz.

- Tempranas (no anticipadas) fallas del sistema – corrección/reemplazo no está lista para sustituir.
- Fallas del Sistema (datos corruptos en informes o pantallas, transacciones pérdidas, entre otros).
- Fallas de interfaces –intercambios de datos no cumplen los requisitos.
- Fallo de la infraestructura regional (energía, telecomunicaciones, sistemas financieros)
- Problemas de implementación (por ejemplo, falta de tiempo o de fondos).
- Aseveraciones falsas o erróneas sobre el cumplimiento, descubiertas demasiado tarde para iniciar las acciones de cumplimiento.

3.3 Identificación de Soluciones:

Actividades importantes a realizar:

- La asignación de equipos de solución para cada función, área funcional o área de riesgo de la organización.
- La asociación de soluciones con cada riesgo identificado
- Comparar los riesgos y determinar los pesos respecto a su importancia crítica en término del impacto de los mismos.
- Clasificar los riesgos.
- La elaboración de soluciones de acuerdo con el calendario de eventos.
- La revisión de la factibilidad de las soluciones y las reglas de implementación.
- La identificación de los modos de implementación y restricciones que afectan a las soluciones.
- La definición e identificación de equipos de acción rápida o equipos de Intensificación por área funcional o de negocios de mayor importancia.
- Sopesar las soluciones y los riesgos y su importancia crítica en lo que respecta a su eficacia y su costo.

3.4 Fallas Genéricas Funcionales de los Sistemas a tener en Consideración.

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

Estos incluyen:

- Autentificación. Un usuario puede inadvertidamente teclear una contraseña en un programa de entrada falso.
- Cifrado. La lista maestra de contraseñas debe ser almacenada, cifrada, lo que a menudo no se hace.
- Implementación. Un diseño bien pensado de un mecanismo de seguridad puede ser implementado de forma improcedente.
- Confianza implícita. Un problema corriente, una rutina supone que otra está funcionando bien cuando, de hecho, debería estar examinando detenidamente los parámetros suministrados por la otra.
- Compartimiento implícito. El sistema puede depositar inadvertidamente información importante del sistema, en un espacio de direcciones del usuario.
- Comunicación entre procesos. El intruso puede usar un mecanismo de SEND/RECEIVE para probar varias posibilidades. Por ejemplo el intruso puede pedir un recurso del sistema y suministrar una contraseña. La información devuelta puede indicar "contraseña correcta", confirmando la contraseña adivinada por el intruso.
- Verificación de la legalidad. El sistema puede no estar realizando una validación suficiente de los parámetros del usuario.
- Desconexión de línea. En tiempos compartidos y en redes, cuando la línea se pierde (por cualquier razón), el sistema operativo debe inmediatamente dar de baja del sistema al usuario o colocar al usuario en un estado tal, que sea necesaria la reautorización para que el usuario obtenga de nuevo el control. Algunos sistemas permiten que un proceso "flote" después de una desconexión de línea. Un intruso puede llegar a obtener el control del proceso y usar cualquier recurso a los que tenga acceso el proceso.
- Descuido del operador. Un intruso puede engañar a un operador y hacer que cargue un paquete de disco con un sistema operativo falso.

- Paso de parámetros por referencia en función de su valor. Es más seguro pasar los parámetros directamente en registros, que tener los registros apuntando a las localidades que contienen los parámetros. El paso por referencia puede llevar a una situación en la cual los parámetros, pueden aún encontrarse en el espacio de direcciones del usuario después de una verificación de la legalidad.

  El usuario podría así suministrar parámetros legítimos, verificarlos, y modificarlos justo, antes de ser utilizados por el sistema.
- Contraseñas. Las contraseñas son, a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse con número máximo (3) de intentos infructuosos.
- Entrampamiento al intruso. Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.
- Privilegio. En algunas sistemas hay demasiados programas con muchos privilegios. Esto es contrario al principio del menor privilegio.
- Confinamiento del programa. Un programa prestado de otro usuario puede actuar como caballo de Troya: puede robar o alterar los archivos del usuario que los prestó.
- Residuos. A menudo el intruso puede encontrar una lista de contraseñas con sólo buscar en una papelera. Los residuos se dejan a veces en el almacenamiento después de las operaciones rutinarias del sistema. La información delicada debe ser siempre destruida antes de liberar o descargar el medio que ocupa (almacenamiento, papel, etc.). Las trituradoras de papel son algo corriente en ese aspecto.
- Blindaje. Una corriente en un cable genera un campo magnético alrededor de él; los intrusos pueden de hecho conectarse a una línea de transmisión o a un sistema de computación sin hacer contacto físico. Puede usarse el blindaje eléctrico para prevenir tales "intrusiones invisibles".
- Valores de umbral. Están diseñados para desanimar los intentos de entrada, por ejemplo. Después de cierto número de intentos inválidos de entrar al sistema, ese

usuario (o el terminal desde donde se intentan las entradas) debe ser bloqueado y el administrador del sistema, advertido. Muchos sistemas carecen de esta característica.

3.5 Ataques Genéricos a Sistemas Operativos

- Asincronismo. Con procesos múltiples que progresan de forma asincrónica, es posible que un proceso modifique los parámetros cuya validez ha sido probada por otro, pero que aún no ha utilizado. Con esto, un proceso puede pasar valores malos a otro, aún cuando el segundo realice una verificación extensa.
- Rastreo. Un usuario revisa el sistema de computación, intentando localizar información privilegiada.
- Entre líneas. Se usa un terminal especial para conectarse a la línea de comunicación mantenida por un usuario dado de alta en el sistema, que está inactivo en ese momento.
- Código clandestino. Se hace un parche en el sistema operativo bajo la pretensión de una depuración. El código contiene trampas que permiten realizar a continuación reentradas no autorizadas al sistema.
- Prohibición de acceso. Un usuario escribe un programa para hacer caer al sistema, poner al sistema en un ciclo infinito, o monopolizar recursos del sistema. Lo que se intenta aquí es el negar el acceso o servicio a los usuarios legítimos.
- Procesos sincronizados interactivos. Los procesos usan las primitivas de sincronización del sistema para compartir y pasarse información entre sí.
- Desconexión de línea. El intruso intenta obtener acceso al trabajo de un usuario después de una desconexión de línea, pero antes de que el sistema reconozca la desconexión.
- Disfraz. El intruso asume la identidad de un usuario legítimo, después de haber obtenido la identificación apropiada por medios clandestinos.
- Engaño al operador. Un intruso inteligente puede, a menudo, engañar al operador del computador y hacer que realice una acción que comprometa la seguridad del sistema.

- Parásito. El intruso utiliza un terminal especial para conectarse a una línea de comunicación. El intruso intercepta los mensajes entre el usuario y el procesador, modifica el mensaje o lo reemplaza por completo.
- Caballo de Troya. El intruso coloca un código dentro del sistema que le permita accesos posteriores no autorizados. El caballo de Troya puede dejarse permanentemente en el sistema o puede borrar todo rastro de sí mismo, después de la penetración.
- Parámetros inesperados. El intruso suministra valores inesperados a una llamada al supervisor, para aprovechar una debilidad de los mecanismos de verificación de la legalidad del sistema.

3.6 Seguridad en Redes

3.6.1 Las Funciones de Seguridad de Red

En el intento de proteger una red de computadoras, existen varias funciones comunes a las cuales deben dirigirse.

a. El Anfitrión Promiscuo

El anfitrión promiscuo es uno de los principales problemas de seguridad y uno de los problemas más urgentes de cualquier red. Si un intruso es paciente, él puede simplemente mirar (con una red debugger o anfitrión promiscuo) que los paquetes fluyen de aquí para allá a través de la red.

No toma mucha programación el análisis de la información que fluye sobre la red.

Un ejemplo simple es un procedimiento de login remoto. En el procedimiento login, el sistema pedirá y recibirá el nombre y contraseña del usuario a través de la red. Durante la transmisión, esta información no es codificada o encriptada de cualquier forma. Una persona

paciente simplemente puede esperar, y así recolectar toda la información que necesita para romper cualquier cuenta.

b. Autenticación

El procedimiento de login remoto ilustra el problema de autenticación.

¿Cómo presenta usted credenciales al anfitrión remoto para probar que usted es usted?.

¿Cómo hace usted esto, de forma que no se repita por el mecanismo simple de una jornada registrada?.

c. Autorización

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

d. Contabilidad

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

3.6.2 Componentes de Seguridad

Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla.

Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. El administrador de la red tal vez tenga que clasificar a los usuarios de la red con el objeto de adjudicarles el nivel de seguridad adecuado.

A continuación se sugiere un sistema en tres niveles:

- Nivel de administración. Aquellos que diseñan, mantienen o ponen en marcha la red. Este debe estar constituido sólo por el administrador o por un pequeño grupo de personal de soporte y administración.
- Usuarios fiables. Aquellos usuarios que cumplen las normas y cuyo trabajo se pueda beneficiar de una mayor libertad de acceso a la red.
- Usuarios vulnerables. Aquellos que muestran falta de competencia, son excesivamente curiosos o beligerantes, o los que por alguna razón no se puede confiar.

3.6.3 Control de Acceso a la Red

- Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Restringir la posibilidad de conectar estaciones mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Identificación para la red con clave de acceso.
- Protección con clave de todas las áreas sensitivas de datos y restricción de acceso a los programas, según su uso.
- Registro de toda la actividad de la estación de trabajo.
- Protección con clave de acceso o bloqueo de todas las operaciones de copia a disquete en las estaciones de trabajo.
- Monitorización de todas las operaciones de copia en disquete en las estaciones de trabajo.

3.6.4 Protección del Servidor

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

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

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

Redes y tolerancia a fallas

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

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

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

4. ESTRATEGIAS

Las estrategias de contingencia - continuidad de los negocios están diseñadas para identificar prioridades y determinar en forma razonable, eficiente y eficaz las soluciones a ser

seleccionadas en primera instancia o los riesgos a ser encarados en primer lugar. Hay que tomar la decisión si se adoptarán las soluciones a gran escala, como las opciones de recuperación de desastres para un centro de datos.

4.1 Actividades Importantes

- La revisión de procesos, flujos, funciones y opciones de importancia crítica.
- La definición de las opciones de contingencia seleccionadas para cada riesgo identificado.
- La revisión y depuración del cronograma maestro. La consolidación de soluciones de acuerdo a las funciones o áreas de negocios más importantes e identificar las estrategias globales.
- La identificación de los impactos de las soluciones y estrategias para ahorrar
  Costos, se deben de considerar varios elementos de costo: como el costo de crear la solución, el costo de implementar la solución, y el costo de mantener vigente dicha solución.
  Debido a que la continuidad de las operaciones de la organización constituye el enfoque primordial, la estrategia de la empresa rige el análisis de costos.
- La obtención de aprobaciones finales para el financiamiento, antes de que se apruebe la solución.
- La identificación de los beneficios es un elemento clave para asegurar que el costo del proyecto esté equilibrado con los retornos reales de la organización

4-2 Preparativos para la Identificación de Soluciones Preventivas

Los puntos que deben ser cubiertos por todos las áreas informáticas y usuarios en General son:

- Respaldar toda la información importante en medio magnético

- Generar discos de arranque para las máquinas dependiendo de su sistema operativo
- Mantener antivirus actualizado, si aplica
- Guardar una copia impresa de la documentación de los sistemas e interfaces, al igual de los planes de contingencia definidos por el resto de las áreas.

4.3 Medida de Precaución y Recomendación

4.3.1 En Relación al Centro de Cómputo

- Es recomendable que el Centro de Cómputo no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados.
- Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor y causar inconvenientes para el equipo de cómputo, puede ser un riesgo para la seguridad del Centro de Cómputo.
- No debe existir materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.
- El acceso al Centro de Cómputo debe estar restringido al personal autorizado.
- Se debe establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.
- El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.
- Se recomienda establecer políticas para la creación de los password y establecer periodicidad de cambios de los mismos.
- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.

4.3.2 Medios de Almacenamientos

4.3.2.1 Recomendaciones para el Mantenimiento de Cintas Magnéticas

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

a. Cintas Magnéticas:

- Temperatura : 4ºC a 32ºC
- Humedad Relativa : 20 % a 80 %
- El ambiente debe contar con aire acondicionado.
- Las cintas deben colocarse en estantes o armarios adecuados.
- Deberá mantenerse alejados de los campos magnéticos.
- Se les debe dar un mantenimiento preventivo en forma periódica a fin de desmagnetizar impurezas que se hayan registrado sobre ellas.

4.3.2.2 Recomendaciones para el Mantenimiento de Discos Magnéticos

Las recomendaciones para el buen mantenimiento de los discos magnéticos son:

- Medios de almacenamiento "delicados", pues si sufren un pequeño golpe puede ocasionar que la información se dañe o producir un CRASH al sistema.
- El cabezal de lectura-escritura debe estar lubricado para evitar daños al entrar en contacto con la superficie del disco.
- Se debe evitar que el equipo sea colocado en una zona donde se acumule calor, ya que el calor interfiere en los discos cuando algunas piezas se dilatan más que otras. Con ello se modifican la alineación entre el disco y los cabezales de lectura-escritura, pudiéndose destruir la

  Información.
- Las ranuras de los ventiladores de refrigeración deben estar libres.
- Se debe evitar, en lo posible, la introducción de partículas de polvo que pueden originar serios problemas.

4.3.2.3 Recomendaciones para el Mantenimiento de los Discos Duros

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

4.3.3 Respecto a los Monitores

- La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección.
- Se recomienda sentarse por lo menos a 60 cm. (2 pies) de la pantalla. No sólo esto reducirá su exposición a las emisiones (que se disipan a una razón proporcional al cuadrado de la distancia), sino que puede ayudar a reducir el esfuerzo visual.
- También manténgase por lo menos a 1 m. o 1.20 m. (3 o 4 pies) del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.
- Finalmente apague su monitor cuando no lo esté usando

3.3.4 Recomendación para el Cuidado del Equipo de Cómputo

Teclado: Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función.

Cpu: Mantener la parte posterior del cpu liberado en por lo menos 10 cm. Para asegurar así una ventilación mínima adecuada.

Mouse: Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste.

Protectores de pantalla: Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.

Impresora: El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel.

5. DOCUMENTACIÓN DEL PROCESO

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

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

- Cuadro de descripción de los equipos y las tareas para ubicar las soluciones a las contingencias.

- La documentación de los riesgos, opciones y soluciones por escrito y en detalle.

La identificación y documentación de listas de contacto de emergencia, la identificación de responsables de las funciones con el fin de garantizar que siempre haya alguien a cargo, y que pueda ser contactada si falla un proceso de importancia

6. PRUEBAS Y VALIDACIONES

6.1 Plan de Recuperación de Desastres

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

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, deben ser planeados y probados fehacientemente.

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

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

6.1.1 Actividades Previas al Desastre

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

Podemos detallar las siguientes Actividades Generales:

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

6.1.2 Actividades Durante el Desastre.

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

- Plan de Emergencias.
- Formación de Equipos.
- Entrenamiento.

6.1.3 Actividades Después del Desastre.

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

- Evaluación de Daños.
- Priorización de Actividades del Plan de Acción.
- Ejecución de Actividades.
- Evaluación de Resultados.
- Retroalimentación del Plan de Acción.

7. IMPLEMENTACIÓN

La fase de implementación se da cuando han ocurrido o están por ocurrir los problemas para este caso se tiene que tener preparado los planes de contingencia para poder aplicarlos. Puede también tratarse esta etapa como una prueba controlada.
De los diferentes tipos de emergencia que pueden ocurrir se pueden encontrar diferentes casos o posibles escenarios:

Emergencia Física:

- **CASO A:** Error Físico de Disco de un Servidor (Sin RAID)
- **CASO B:** Error de Memoria RAM
- **CASO C:** Error de Tarjeta(s) Controladora(s) de Disco
- **CASO D:** Caso de Incendio Total
- **CASO E:** Caso de Inundación
- **CASO F:** Caso de Fallas de Fluido Eléctrico

Emergencias Lógicas de Datos:

- **CASO A:** Error Lógico de Datos
- **CASO B:** Caso de Virus

8. MONITOREO

El correcto Monitoreo nos dará la seguridad de poder reaccionar en el tiempo preciso y con la acción correcta.

8.1 Actividades principales a realizar:

- Desarrollo de un mapa de funciones y factores de riesgo.
- Establecer los procedimientos de mantenimiento para la documentación y la rendición de informes referentes a los riesgos.

- Revisión continúa de las aplicaciones.
- Revisión continua del sistema de backup

  Revisión de los Sistemas de soporte eléctrico del Centro de Procesamiento de Datos

8.1 Prueba de Plan de Contingencia

Con el objeto de demostrar su habilidad, de mantener la continuidad de los procesos críticos de la entidad, todos los planes deben ser probados

Las pruebas se efectúan simultáneamente a través de múltiples departamentos, incluyendo entidades comerciales externas.

Realizando pruebas se descubrirán elementos operacionales que requieren ajustes para asegurar el éxito en la ejecución del plan, de tal forma que dichos ajustes perfeccionen los planes preestablecidos.

Objetivos

El objetivo principal, es determinar si los planes de contingencia Son capaces de proporcionar el nivel deseado de apoyo a la sección o a los procesos críticos de la empresa, probando la efectividad de los procedimientos expuestos en el plan de contingencias.

8.2 Procedimientos Recomendados para las Pruebas del Plan de Contingencias,

1. Niveles de Prueba

Se recomiendan tres niveles de prueba:

- Pruebas en pequeñas unidades funcionales o divisiones.
- Pruebas en unidades departamentales
- Pruebas interdepartamentales o con otras instituciones externas.

2. Métodos para Realizar Pruebas de Planes de Contingencia

a) Prueba Específica

Consiste en probar una sola actividad, entrenando al personal en una función específica, basándose en los procedimientos estándar definidos en el Plan de Contingencias. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

b) Prueba de Escritorio

Implica el desarrollo de un plan de pruebas a través de un conjunto de preguntas típicas (ejercicios).

Características:

La discusión se basa en un formato preestablecido.
Esta dirigido al equipo de recuperación de contingencias.
Permite probar las habilidades gerenciales del personal que tiene una
Mayor responsabilidad

Los ejercicios de escritorio, son ejecutados por el encargado de la prueba y el personal responsable de poner el plan de contingencias en ejecución, en una situación hipotética de contingencia. Un conjunto de preguntas se pedirán que resuelva el personal. El encargado y el personal utilizarán el plan de contingencias para resolver las respuestas a cada situación. El encargado contestará a las preguntas que se relacionan con la disponibilidad del personal Entrenado, suficiencia de los recursos, suficiencia de máquinas, y si los requerimientos necesarios están a la mano. Los ajustes serán hechos al plan o al ambiente determinado durante esta fase si cualquier parte del plan no cumple con los objetivos propuestos.

c) Simulación en Tiempo Real

Las pruebas de simulación real, en un departamento, una división, o una unidad funcional de la empresa está dirigido una situación de contingencia por un período de tiempo definido.

- Las pruebas se hacen en tiempo real
- Es usado para probar partes específicas del plan
- Permite probar las habilidades coordinativas y de trabajo en equipo de los Grupos asignados para afrontar contingencias.

3 Preparaciones Pre Prueba

- Repasar los planes de contingencia seleccionados para probar.
- Verificar si se han asignado las respectivas responsabilidades.
- Verificar que el plan este aprobado por la alta dirección de la institución.
- Entrenar a todo el personal involucrado, incluyendo orientación completa de los objetivos del plan, roles, responsabilidades y la apreciación global del proceso.
- Establecer la fecha y la hora para la ejecución de la prueba.
- Desarrollar un documento que indique los objetivos, alcances y metas de la prueba y distribuirlo antes de su ejecución.
- Asegurar la disponibilidad del ambiente donde se hará la prueba y del personal esencial en los días de ejecución de dichas pruebas.
- No hacer «over test»—la meta es aprender y descubrir las vulnerabilidades, no generar fracaso y frustración.

4 Comprobación de Plan de Contingencias

La prueba final debe ser una prueba integrada que involucre secciones múltiples e Instituciones externas.

5 Mantenimiento de Plan de Contingencias y Revisiones

Las limitaciones y problemas observados durante las pruebas deben analizarse Planteando alternativas y soluciones, las cuales serán actualizadas en el Plan de Contingencias.

Este formato se propone para describir el escenario real donde se hará la prueba.
Documentará el día de la semana y la hora (si es necesario) de ocurrencia del Acontecimiento. La "Descripción del Evento/Mensaje" define los eventos del Incidente presentado en el departamento, los cuales se deben solucionar. Las soluciones deben ser coincidentes con los planes de contingencia previamente aprobados. El 'ítem #' debe ser utilizado por los observadores y los evaluadores para realizar identificaciones, dar respuestas a los acontecimientos y a los mensajes específicos mientras estos ocurren.

6 Entorno de las Pruebas del Plan de Contingencias:

- Pruebas de objetivos y alcances.
- Pruebas metodológicas.
- Precisar equipos y recursos.
- Demanda de personal capacitado.
- Detallar itinerarios y localizaciones.
- Control del Proceso.
- Objetivos trazados a partir del control.
- Control de la evaluación y observaciones.

7 Obligación de Mitigar los Daños

Es dable mencionar que si los sistemas de Información de una entidad fallan y esto da como resultado pérdidas o daños, entonces la entidad tiene la obligación de evitar la acumulación innecesaria de daños adoptando las medidas necesarias para mitigarlos.
De igual manera, si ocurren pérdidas a raíz de las acciones de terceros, es posible que la entidad no recupere los daños que a sabiendas permitió que aumentaran. En otras palabras, las entidades no deben confiar en el hecho de que inicialmente no fue su culpa y simplemente suponer que la parte culpable se responsabilizará de todas las pérdidas y daños resultantes.

La compañía, entidad u organización, debe adoptar algún tipo de acción para minimizar el impacto sobre sus negocios, y los daños a la propiedad, resultantes de una falla del sistema de información.

En la práctica, un plan de contingencia puede y debe ser visto como una herramienta para cumplir con esta obligación legal.

Meta: Documentación de un Plan

Un plan de contingencia tiene un valor limitado desde el punto de vista comercial o legal, si no fue redactado por escrito y si no se mantiene adecuadamente en lugares de fácil acceso para el personal clave.

Generalmente, para propósitos legales para evitar y defender cualquier alegato de negligencia o falta de cuidado debido es de importancia crítica que los planes de contingencia sean revisados apropiadamente para que se adecuen al sistema de información, con los jefes de equipo y los funcionarios y/o los miembros de las juntas directivas y además que dichas acciones sean tomadas con una anticipación suficiente ante cualquier problema.

CONCLUSION

El resguardo de la información y la continuidad de las operaciones ante eventualidades o desastres, constituye una de las principales estrategias que deben desarrollar y procurar las organizaciones modernas ya sean públicas o privadas, ya que de ello depende en la mayoría de los casos, la continuidad o cese de los servicios entregados por la organización a la comunidad, especialmente ante eventos inesperados como desastres o contingencias.

Por lo anterior el desarrollo de esta investigación ha permitido mostrar que en la actualidad las entidades públicas, si bien han presentado antecedentes de pérdida de información crítica y limitaciones en continuidad de los servicios, las estrategias preventivas y de respuestas generadas ante estos eventos, han resultado ser acciones aisladas, poco efectivas y que no obedecen a la instalación de planes de contingencias y de procesos de resguardo de la información.

En este sentido destaca la total ausencia de Planes de Contingencia en las organizaciones estudiadas, si bien en su gran mayoría los servicios cuentan con un plan de emergencia, este no identifica los riesgos asociados, alternativas de solución en caso de fallas, ni plan de recuperación de la información.

En relación a la evaluación realizada al conocimiento de los sistemas de inventario, las organizaciones dan cuenta de la presencia de inventarios de Hadware y Software y conocimiento respecto de estos, sin embargo un grupo minoritario utiliza criterios de evaluación de los elementos críticos y ausencia en la identificación de los riesgos para el negocio de cada entidad.

En cuanto al cumplimiento o adecuación de las organizaciones a las normas y estándares de calidad y buenas prácticas de los sistemas TI establecidos por la comunidad internacional, es posible señalar en relación a la Seguridad Física, la ausencia de Planes de Prevención en caso de desastres, escases en la instalación de Políticas de Seguridad, presentando en esta línea un

grupo minoritario de entidades que documenta las políticas de seguridad, y que implementa un proceso de difusión y sensibilización del RRHH respecto de los métodos de acción frente a la ocurrencia de desastres. La Seguridad Lógica de igual forma presenta falencias importantes en las organizaciones estudiadas, como no utilizar protocolos estandarizados para la creación de contraseñas, ausencia de procesos de mantenimiento de licencias, ni procedimientos sistemáticos de cambios de contraseña para el RRHH cada cierto tiempo. En cuanto a la Seguridad en Redes destaca la falta de utilización de estándares o normas en la instalación de cableado, la escases de reguladores de emergencia de PC, constituyendo un bajo porcentaje de servicios que cuenta con un sistema de protección de cargas. En esta misma línea la Seguridad en Sistemas posee insolvencias relevantes como no realizar adecuadamente la documentación del sistema, manuales de usuario, mantenimiento y recomendaciones de seguridad.

Finalmente y como elemento fundamental para el levantamiento de un Plan de Contingencia para el Resguardo de la Información, lo constituye la Evaluación de Riesgos de Seguridad de la Información, en la cual la totalidad de las organizaciones públicas estudiadas presentó una evaluación de Riesgo de medio a Alto, lo que significa que ante las probabilidades de amenaza que presenta cada servicio la magnitud de daño en pérdida de la información y cese de funciones es considerada alta.

Estos resultados releva la importancia de contar con procedimientos documentados en esta línea, con responsables y con el conocimiento claro y protocolizado de cómo actuar en caso de una contingencia como parte fundamental de los procesos de un área de tecnología que mantendrá a la organización, entidad u empresa en funcionamiento, ya que la única misión de un Plan de Contingencia Tic es salvaguardar el activo más importante de la organización: la Información, con el objeto que cumpla con los objetivos de confidencialidad, integridad y disponibilidad.

Por ende y como se ha visto reflejado en esta investigación se hace necesario un cambio cultural acerca de la importancia de la seguridad de la información por parte de Directores, Alcaldes y Funcionarios. Esto significa que las entidades deben invertir recursos, sean humanos, financieros y tecnológicos que favorezcan acciones preventivas y de intervención

ante este tipo de situaciones. En este sentido se debe fomentar y potenciar en las entidades públicas la instalación de prácticas que den cuenta de la implementación, desarrollo y mantenimiento de un plan de contingencia y recuperación que garantice la continuidad de la operación, resguardando la información ante una contingencia y que además permita y asegure la recuperación de la información más crítica de la organización en el menor tiempo posible.

BIBLIOGRAFIA

- Educación Tecnológica (editorial averbuj)
- Cobit 4.1 (Isaca)
- Itil v.3
- Implantación de un sistema de gestión de seguridad de la información según ISO 27001, (Merino Bada; Cañizares Ricardo), editorial FC.

LINKOGRAFIA

- www.iso27000.es/glosario.html
- www.elespectador/noticia/elmundo/el-hombre-robo-informacion-financiera-de-20-millones-articulo-470037),
- www.latercera.com/noticia/nacional/2014/03/680-570673-9-registro-civil-denuncia-copia-irregular-de-base-de-datos-de-carnes-y-pasaportes.shtml),
- www.eoi.es/blogs/innovando/
- http://calidadtic.blogspot.com/2011/01/como-hacer-un-plan-de-contingencia.html
- http://www.ongei.gob.pe/seguridad/seguridad2_archivos/Lib5131/Libro.pdf
- http://ceur-ws.org/Vol-488/paper13.pdf
- http://searchdatacenter.techtarget.com/es/cronica/Pasos-para-un-Plan-de-Recuperacion-de-Desastres-DR

ANEXOS

Checklist de Seguridad Física

Nro.	Criterio	Proceso ITIL	Norma / Estándar	Cumple el criterio Si	Cumple el criterio No	Observaciones
1	¿Existen políticas de seguridad de la información?	Libro 2 Gestión de la seguridad de la información	ISO/IEC 27002			
2	¿Cuentan con plan de prevención en caso de algún desastre?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-003-SEGOB-2008			
3	¿Cuenta con extintores dentro de la organización?	Libro 1 Gestión financiera	NOM – 002 – STPS – 2000			
4	¿Los extintores con que se cuentan son de fuego clase "C"?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-100-SPTS-1994			
5	¿Tiene políticas de seguridad de los equipos sobre alimentos, líquidos o cualquier tipo de sustancia que dañe los quipos?	Libro 2 Gestión de la continuidad de los servicios de TI	ISO/IEC 17799			
6	¿Cuenta con señalamientos de rutas de evacuación?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-003-SEGOB-2008			

7	¿Están documentadas las políticas de seguridad?	Libro 2 Gestión de la seguridad de la información	ISO/IEC 27002			
8	¿El personal conoce métodos y procedimientos parahacer frente a las emergencias o riesgos por desastres?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-003-SEGOB-2008			
9	¿Cuenta con señalamientos que ayuden a identificar zonas restringidas, donde solo personal autorizado pueda ingresar?	Libro 2 Gestión de la seguridad de la información	NOM-003-SEGOB-2008			
10	¿Existe un señalamiento que obligue al registro de la persona para el acceso a las instalaciones?	Libro 2 Gestión de la seguridad de la información	NOM-003-SEGOB-2008			
11	¿Se le da un seguimiento a las pólizas de garantías de los equipos utilizados en la organización?	Libro 2 Gestión de la continuidad de los servicios de TI	ISO/IEC 17799			
12	¿Existe un control de las pérdidas de información dentro de la organización?	Libro 2 Gestión de la seguridad de la información	ISO/IEC 17799			
13	¿Cuenta con alarmas de incendio?	Libro 2 Gestión de la seguridad de la información	NOM-002-STPS-2000 Justificación 8			

14	¿Las áreas de trabajo se encuentran delimitadas o seccionadas?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM – 001 – STPS – 1999			
15	¿Las zonas donde exista alto voltaje se encuentran señalizadas?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-003-SEGOB-2008			
16	¿Las condiciones eléctricas, de iluminación y climáticas son adecuadas para el buen funcionamiento de los equipos de cómputo?	Libro 2 Gestión de la continuidad de los servicios de TI	ISO/IEC 17799			
17	¿Cuenta con las herramientas necesarias para el mantenimiento a los equipos?	Libro 1 Gestión financiera	ISO/IEC 17799 Justificación 12			
18	¿Se asigna al personal una carta responsiva por el equipo que está utilizando?	Libro 2 Gestión de la seguridad de la información	ISO/IEC 27002.			
19	¿Se documenta la entrega-recepción a la organización por parte de los empleados que dejan la organización?	Libro 2 Gestión de la seguridad de la información	ISO/IEC 27002. Justificación 18			
20	¿Cuenta con cámaras monitoreando el site de la organización?	Libro 1 Gestión financiera	HDCCTV			

Checklist de Seguridad Lógica

Nro	Criterio	Proceso ITIL	Norma / Estándar	Cumple el criterio		
				Si	No	
1	¿Existen metodologías de respaldo de información?	Libro 2 Gestión de la seguridad de la información	ISO/IEC 17799			
2	¿Se realizan respaldos de información periódicamente?	Libro 2 Gestión de la seguridad de la información	ISO/IEC 17799			
3	¿Existe un administrador de sistemas que controle las cuentas de los usuarios?	Libro 4 Gestión de Acceso a los Servicios TI	ISO/IEC 17799			
4	¿Existe algún estándar para la creación de contraseñas?	Libro 2 Gestión de la seguridad de la información	Data Encryption Standard (DES)			
5	¿Las contraseñas cuentan con letras, números y símbolos?	Libro 2 Gestión de la seguridad de la información	ISO/IEC 17799			
6	¿Se obliga, cada cierto tiempo a cambiar la contraseña?	Libro 2 Gestión de la seguridad de la información	ISO/IEC 17799			
7	¿La organización cuenta con un proceso para dar mantenimiento preventivo al software?	Libro 2 Gestión de la continuidad de los servicios de TI	IEEE1219			

8	¿La organización cuenta con un proceso para dar mantenimiento correctivo al software?	Libro 2 Gestión de la continuidad de los servicios de TI	IEEE1219			
9	¿Se tienen software antivirus instalados en los equipos de cómputo?	Libro 2 Gestión de la seguridad de la información	ISO 17799			
10	¿Cuentan con antivirus actualizado?	Libro 3 Gestión de cambios	ISO 17799			
11	¿hay instalados anti malware en los equipos de cómputo?	Libro 3 Gestión de cambios	SGSI SISTESEG			
12	¿Cuenta con licencias de software?	Libro 3 Gestión de cambios	ISO/IEC 19770			
13	¿Existe un proceso para mantener las licencias actualizadas?	Libro 3 Gestión de cambios	ISO/IEC 19770			
14	¿Existe un proceso para adquirir nuevas licencias?	Libro 3 Gestión de cambios	ISO/IEC 19770			
15	¿Se sanciona al integrante del departamento si instala software no permitido?	Libro 2 Gestión de la seguridad de la información	NEG001			
16	¿Los usuarios de bajo nivel tienen restringido el acceso a las partes más delicadas de las aplicaciones?	Libro 4 Gestión de Acceso a los Servicios TI	ISO/IEC 17799 Justificación 5			

17	¿Realizan mantenimiento preventivo al equipo de cómputo?	Libro 2 Gestión de la Disponibilidad	NOM-004-STPS-1999			
18	¿Realizan mantenimiento correctivo al equipo de cómputo?	Libro 2 Gestión de la Disponibilidad	NOM-004-STPS-1999			
19	¿El equipo de cómputo cuenta con suficiente espacio en HD en función de los servicios que otorga?	Libro 2 Gestión de la Disponibilidad	ISO/IEC 20000			
20	¿El equipo de cómputo cuenta con suficiente memoria RAM en función de los servicios que otorga?	Libro 2 Gestión de la Disponibilidad	ISO/IEC 20000			
21	¿La velocidad del procesador es el adecuado para los programas que son utilizados en los equipos?	Libro 2 Gestión de la Disponibilidad	ISO/IEC 20000			

Checklist de Seguridad en Redes

Nro	Criterio	Proceso ITIL	Norma / Estándar	Cumple el criterio		Observaciones
				Si	No	
1	¿Las salidas de corriente eléctrica son trifásicas?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-001-SCFI-1993			
2	¿Los interruptores de energía están debidamente protegidos y sin obstáculos para alcanzarlos?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-001-SCFI-1993			
3	¿La instalación eléctrica del equipo de cómputo es independiente de otras instalaciones?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-001-SCFI-1993			
4	¿Los firewalls están configurados conforme a las necesidades de la organización?	Libro 2 Gestión de la seguridad de la información	IEEE 802.10			
5	¿El acceso de la red inalámbrica es a través de contraseñas?	Libro 2 Gestión de la seguridad de la información	IEEE 802.11			
6	¿El tráfico de la red por medio inalámbrico se encuentra protegido (encriptado)?	Libro 2 Gestión de la seguridad de la información	IEEE 802.11			

7	¿Los dispositivos inalámbricos intermediarios están físicamente protegidos?	Libro 2 Gestión de la seguridad de la información	IEEE 802.11			
8	¿Cada PC cuenta con un regulador de energía?	Libro 1 Gestión financiera	NOM-001-SCFI-1993			
9	¿El cableado del edificio es accesible para una revisión física?	Libro 2 Gestión de la continuidad de los servicios de TI	ANSI/EIA/TIA-569			
10	¿Los cables de equipos se encuentran debidamente aislados del paso de personas?	Libro 2 Gestión de la continuidad de los servicios de TI	TIA/EIA-568			
11	¿Cuenta con administración de red y documentación cuando se han hecho cambios en la misma?	Libro 2 Gestión de la continuidad de los servicios de TI	ANSI/TIA/EIA-606			
12	¿Se apega a algún estándar para asignar el cableado eléctrico al inmueble?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-001-SCFI-1993			
13	¿Se cumple con el estándar de tierra física según requisitos establecidos en las normas?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-022-STPS-1999 ANSI/TIA/EIA-607			

14	¿La topología de cableado está definida bajo un estándar establecido?	Libro 2 Gestión de la continuidad de los servicios de TI	TIA/EIA-568			
15	¿El cableado cuenta con una debida administración en cuanto a la identificación de etiquetas?	Libro 2 Gestión de la continuidad de los servicios de TI	ANSI/TIA/EIA-606			
16	¿Los tipos de cables, distancias, conectores, Arquitecturas, terminaciones de cables y características de rendimiento están definidos por estándar?	Libro 2 Gestión de la continuidad de los servicios de TI	TIA/EIA-568			
17	¿Cuentan con un sistema de protección de descargas electro atmosféricas para el área de servidores?	Libro 2 Gestión de la continuidad de los servicios de TI	NOM-022-STPS-1999			

Checklist de Seguridad en Sistemas

	Criterio	Proceso ITIL	Norma / Estándar	Cumple el criterio Si	Cumple el criterio No	Observaciones
1	¿Las bases cuentan con un modelo o esquema de organización de los datos?	Libro 2 Gestión de la seguridad de la información	ISO/IEC 27001			
2	¿Existe backup para respaldar información de las bases de datos?	Libro 2 Gestión de la seguridad de la información	ISO 9001			
3	¿El cuentan con un administrador del sistema?	Libro 2 Gestión de la seguridad de información	ISO 9001			
4	¿Cuenta con una póliza de seguridad en caso de fallos?	Libro 2 Gestión de la continuidad de los servicios de TI	ISO 9001			
5	¿Las bases de datos son seguras?	Libro 2 Gestión de la seguridad de información	ISO 9001			
6	¿El sistema fue creado bajo un modelo para la mejora y evaluación de los procesos de desarrollo y mantenimiento de sistemas?	Libro 3 Gestión de entregas y despliegues	ISO 9001			

7	¿Se cuenta con personal especializado para que monitoree el rendimiento del sistema?	Libro 2 Gestión de la seguridad de la información	ISO 9001			
8	¿Se realiza adecuadamente la documentación del sistema, manuales de usuario, mantenimiento y recomendaciones ?	Libro 3 Gestión de entregas y despliegues	ISO 9001			
9	¿Se utiliza encriptación para la información que se almacena en las bases de datos?	Libro 2 Gestión de la seguridad de la información	ISO 9001			
10	¿El sistema es escalable para nuevas aplicaciones?	Libro 3 Gestión de entregas y despliegues	ISO 9001			

Fuente: http://auditoriasistemas10c.blogspot.com/

CHECKLIST DEL DICCIONARIO DE DATOS	*SÍ*	*NO*	*N/A*
CONOCIMIENTO DEL SISTEMA: INVENTARIO			
¿Existe un inventario en la entidad de Sistemas, Hardware y Datos?			
¿Ha hecho revisar el inventario por un especialista (auditor, consultor, experto en informática...) *externo a la empresa*?			
¿Se sabe quiénes son los propietarios de los elementos del inventario?			
¿Se sabe quiénes son los usuarios de los elementos del inventario?			
¿Existe un criterio para valorar cuáles son los elementos críticos del inventario?			
¿Se distingue en ese criterio entre: Riesgos para el negocio, riesgos para el servicio prestado a los clientes y riesgo de parálisis de la gestión de la Compañía?			
¿Han validado ese criterio los jefes de Gestión de la Empresa y los jefes de Informática?			
¿Se ha realizado, por lo tanto, un ranking de los elementos más críticos?			
¿Se van a comenzar las pruebas y actualizaciones, por lo tanto, siguiendo el orden del ranking?			

Fuente: Checklist Repositorio. Base de Datos

CONOCIMIENTO DEL SISTEMA: PLANES DE CONTINGENCIA	SI	NO	NoSabe
¿Existe un plan de contingencia para el área TI?			
¿**Existe algún plan de emergencia u otro que garantice el buen funcionamiento de la entidad?**			
¿**En el plan se identifican todos los riesgos asociados, fallas e interrupciones**?			
¿Contempla el plan identificación de Alternativas, o soluciones en caso de fallas?			
¿El plan contempla Estrategias u otras opciones de soluciones, ya sea manual o informática?			
¿**Existe un manual documentado de los procesos y etapas del plan?**			
¿**Existe un plan de recuperación de desastre**?			
¿La implantación del plan se efectuó debido a problemas detectados o que ya hayan actualmente?			
¿Se efectuaron las pruebas a la seguridad Física, Lógica, Redes y Sistemas, documentando sus resultados?			

Fuente: Elaboración Propia