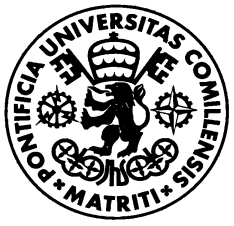

UNIVERSIDAD PONTIFICIA COMILLAS

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

INGENIERO EN INFORMÁTICA

PROYECTO FIN DE CARRERA

PLAN GENERAL DE SEGURIDAD DE UNA EMPRESA

AUTOR: DAVID DE DOMPABLO FANTOVA

MADRID, Septiembre de 2008

Autorizada la entrega del proyecto del alumno:

David de Dompablo Fantova

EL DIRECTOR DEL PROYECTO

Mateo Camps Llufríu

Fdo.: Fecha: 01/09/2008

Vº Bº del Coordinador de Proyectos

Eduardo Alcalde Lancharro

Fdo.: Fecha: 12/09/2008

A mi familia y amigos, por toda la ayuda que me han prestado y apoyarme siempre en los momentos difíciles.
Gracias a todos.

RESUMEN DEL PROYECTO

Está demostrado que la información y los sistemas informáticos son las posesiones más importantes que disponen la mayoría de las organizaciones. Esto supone que la pérdida de dicha información podría suponer una catástrofe para la empresa, perdiendo así la información de sus clientes, la lógica de negocio y un sin fin de información vital, suponiendo daños irreparables para la empresa.

Este proyecto consiste en la realización de un plan general de seguridad, que preserve de numerosos inconvenientes dicha información, en el que se desarrollan conjuntamente un plan de contingencias y otro de recuperación, ya que la existencia de uno solo, sin el apoyo del otro plan, sería un error muy grande, ya que cuando el plan de contingencias falla, el plan de recuperación entra en acción.

Asegurar la información al completo sería algo muy caro, además de imposible. Por tanto, se puede asegurar que en todo momento existirán posibilidades de riesgo, y que en algún momento se puede llegar a producir un desastre sin conseguir evitarlo. Estos desastres pueden causar daños en mayor o menor medida a las empresas y a sus sistemas.

Para intentar evitar que se produzcan dichos desastres, como sus consecuencias, son necesarias tomar unas medidas de seguridad estrictas, por ello el objetivo principal de este proyecto es elaborar un plan general de seguridad que garantice la continuidad de los sistemas de información así como los procesos de negocio de la compañía.

Para elaborar el plan de seguridad inicialmente el autor llevó a cabo un estudio del entorno existente, recogió y analizó todos los requerimientos de la empresa, los procesos necesarios de tecnologías de información en la compañía, hizo un estudio de las metodologías de planes de contingencias existentes para implantar la más adecuada, llevó a cabo un análisis de riesgos e hizo un estudio pormenorizado de la información que genera la compañía, de cara a implantar políticas de seguridad en los datos y backup de los mismos.

Después de este análisis se llevo a cabo el inventariado de equipos informáticos para así poder conocer en todo momento como se encuentra el parque de terminales de la entidad. A continuación se determinaron las normativas de seguridad tanto físicas como lógicas que se deben cumplir dentro de la compañía en cuanto al acceso a la información. En este apartado se han englobado temas como políticas de seguridad física en el edificio, control de acceso, sistemas de seguridad, control de contraseñas, controles físicos, controles del software, etc.

Una vez definidas las normativas internas de seguridad, se procedió a la realización del plan de respaldo de copias de la empresa, en este plan se ha definido la periodicidad de realización de las copias, el procedimiento de realización de las mismas y el procedimiento de recuperación de los datos.

Por último, se llevó a cabo el análisis de los diversos riesgos a los que están expuestos los sistemas de información de la entidad, este capítulo ha sido la parte del proyecto que más horas se le ha dedicado. En este análisis, primeramente, se ha realizado una evaluación de los riesgos naturales, riesgos de corte de suministro, riesgos inducidos y riesgos informáticos, definiendo tres casos posibles para cada riesgo que se pueda presentar. Una vez realizada esta evaluación, se han definido una serie de medidas preventivas para evitar que los posibles riesgos se materialicen. Para acabar con este análisis se ha llevado a cabo un plan de acción con las medidas correctoras que se deben adoptar en caso de que el riesgo se materialice.

ABSTRACT

It has been proved that information and computer systems are the most important possessions the majority of the organizations have at their disposal. This means that the loss of the mentioned information could involve a catastrophe for the company, therefore losing the information of his clients, business logic and a great amount of vital information, causing irreparable damages for the company.

This project involves the accomplishment of a general safety plan, which would preserve the mentioned information from numerous disadvantages, in which a contingencies plan and another recovery one are developed at the same time, since the existence of either of them without the support of the other, would be a very big mistake, because when the contingencies plan fails, the recovery plan comes into action.

To save the complete information would be very expensive, besides impossible. Therefore, it is possible to assure that there will always exist possibilities of risk, and that at any moment a disaster could take place without managing to avoid it. These disasters can cause damages to a greater o lesser extent to the companies and to its systems.

In order to try to avoid the mentioned disasters, and their consequences, it is necessary to adopt a few important and strict safety measures. In that for, the main aim of this project is to elaborate a general safety plan that would guarantee the continuity of information systems as well as the business processes of the company.

Initially, to elaborate the safety plan, the author carried out a study of the existing environment, gathered and analyzed all the requirements of the company, the necessary information technologies processes in the company, did a study of the existing contingency plan methodologies in order to implement the most suitable, carried out an analysis of risks and did a detailed study of the information generated by the company, in order to implement safety policies in the data and their backup.

After this analysis, an inventory was made about the computer equipments in order to know the status of the terminal collection of the organization.

Next, both physical and logical safety regulations related to information accessibility, which were mandatory inside the company, were determined. This section includes subjects such as physical safety policies inside the building, access control, security systems, password control, physical control, software control, etc.

Once defined the internal safety regulations, the plan of backup copies of the company was accomplished. The periodicity of accomplishment of the backups, their procedure of accomplishment and the data recovery procedure are defined in this plan.

Finally, the analysis of the diverse risks to which the company information systems are exposed was carried out. This is the section of the project that has required most part of the time. In this analysis, in first instance, an environmental risk, supply loss risks induced risks and computing risks measurement has been carried out, defining the three possible cases involving each risk that could arise. Once performed this evaluation, a couple of preventive measures in order to avoid risks to come up have been defined. To finish with this analysis, an action plan with the measures that must be adopted in case that the risk comes up, in order to correct the situation, is carried out.

ÍNDICE DEL PROYECTO

CAPITULO 1 "PLAN DE GESTIÓN DEL PROYECTO" 1

1.1. Definición del proyecto 2

1.2. Ámbito y alcance del proyecto 2

1.3. Objetivos del proyecto 3

CAPITULO 2 "ANÁLISIS DE LA EMPRESA" 5

2.1. Introducción 6

2.2. Metodología 6

2.3. Servicios 7

2.4. Organigrama 8

2.5. Arquitectura Técnica 12

2.6. Arquitectura Hardware 13

CAPITULO 3 "DETERMINACIÓN DE APLICACIONES Y DATOS" 18

3.1. Determinación de aplicaciones y datos críticos 19

3.2. Aplicaciones críticas para la empresa 21

CAPITULO 4 "SEGURIDAD FÍSICA Y LÓGICA DE LA EMPRESA" 23

4.1. Seguridad Física 24

4.1.1. Seguridad física de los edificios 24

4.1.2. Control de acceso 26

4.2. Seguridad Lógica 27

4.2.1. Seguridad en el acceso a la información 27

4.2.2. Seguridad en las estaciones de trabajo 33

4.2.3. Integridad de la información 35

CAPITULO 5 "SOPORTE DE LA INFORMACIÓN" 36

5.1. Copias de seguridad 37

5.2. Soporte de almacenamiento 42

5.3. Guardado de la información 44

5.4. Acceso a la información 46

5.5. Restauración de datos 47

CAPITULO 6 "RIESGOS Y MEDIDAS" 48
6.1. Análisis de Riesgos 49
6.2. Identificación de los riesgos 53
6.3. Sistema de valoración de riesgos 56
6.4. Evaluación de Riesgos 58
6.4.1. Riesgos Naturales 58
6.4.2. Riesgos en el fallo de suministro 69
6.4.3. Riesgos inducidos 76
6.4.4. Riesgos informáticos 89
6.5. Medidas preventivas y correctoras 111
6.5.1. Medidas para riesgos naturales 111
6.5.2. Medidas para riesgos en el fallo de suministro 115
6.5.3. Medidas para riesgos inducidos 118
6.5.4. Medidas para riesgos informáticos 122
CAPITULO 7 "CENTRO DE ATENCIÓN A USUARIOS (CAU)" 132
7.1. Gestión de incidencias 133
7.2. Plan de Acción 138
CAPITULO 8 "PLANIFICACIÓN REAL DE LAS ACTIVIDADES" 145
CAPITULO 9 "CONCLUSIONES" 148
CAPITULO 10 "BIBLIOGRAFÍA" 151
CAPITULO 11 "ANEXOS" 154
11.1. ANEXO A. Valoración real del proyecto 155
11.2. ANEXO B. Índice de tablas 156
11.3. ANEXO C. Índice de Figuras 159

1

PLAN DE GESTIÓN DEL PROYECTO

1.- PLAN DE GESTIÓN DEL PROYECTO.

1.1.- DEFINICIÓN DEL PROYECTO.

El siguiente proyecto es el resultado del desarrollo de un plan de contingencias y recuperación.

Para la realización del mismo se ha contado con la colaboración de profesionales expertos en las distintas áreas técnicas.

La seguridad de las tecnologías de la información en cualquier sector de actividad, se materializa en un plan de contingencias y recuperación, que debe contemplar las necesidades reales de la Compañía, ser eficaz y lograr un coste económico controlado.

1.2.- ÁMBITO Y ALCANCE DEL PROYECTO.

A medida que las empresas dependen de los ordenadores y de las redes para manejar sus actividades, la disponibilidad de los sistemas informáticos se ha vuelto crucial. Las empresas necesitan un alto nivel de disponibilidad, ya que les resultaría extremadamente difícil funcionar sin los recursos informáticos.

La interrupción prolongada de los servicios informáticos puede conllevar a grandes pérdidas financieras. Lo más grave es que se puede perder la credibilidad del público o de los clientes y, como consecuencia, la empresa puede terminar en un fracaso total.

En caso de desastre, un seguro puede cubrir los costes materiales de una organización, pero no serviría para recuperar el negocio ya que no ayudará a conservar a los clientes y, en la mayoría de los casos, no proporcionará fondos por adelantado para mantener el funcionamiento del negocio hasta que se haya recuperado.

En un estudio realizado se ha demostrado que más del 60% de las empresas que sufren un desastre y que no tiene un plan de recuperación ya en funcionamiento, abandonarán el negocio en un par de años. Mientras vaya en aumento la dependencia de la disponibilidad de los recursos informáticos, este porcentaje seguramente crecerá.
Por lo tanto, la capacidad para recuperarse con éxito de los efectos de un desastre dentro de un periodo determinado debe ser un elemento crucial en un plan de seguridad de una organización.

La reanudación de las actividades ante un desastre es una de las situaciones más difíciles con las que una organización puede enfrentarse. Tras un desastre, es probable que no haya posibilidades de regresar al lugar de trabajo o que no se disponga de ninguno de los recursos necesarios. Incluso, es posible que no se pueda contar con todo el personal. La preparación es la clave del éxito para enfrentarse a los problemas.

1.3.- OBJETIVO DEL PROYECTO.

El objetivo del plan es garantizar la continuidad de los servicios informáticos ante la aparición de:

- Una contingencia que afecte a los elementos de proceso de datos.
- Incidencias que afecten a la red de gestión de los equipos propiedad de la Compañía.

Plan de Seguridad

Figura 1.1.-Plan general de seguridad.

En el estudio y puesta a punto del plan de seguridad informática se distinguen dos áreas:

- Seguridad de la Información.
- Plan de Contingencias y Recuperación.

Sin que pueda establecerse un límite nítido entre ambas áreas.

Para ello la primera parte del proyecto tiene como objetivo fundamental el estudio de vulnerabilidades, que afecta a la seguridad general de la empresa con el objetivo de garantizar la 'continuidad del servicio informático'.

En síntesis el proyecto agrupa los estudios enfocados a determinar:

- Qué proteger (Sistemas de Información, hardware, edificios, personas, etc.).
- Contra qué (Riesgos potenciales que afectan a las instalaciones, personas, información, etc.).

2

INTRODUCCIÓN A LA EMPRESA

2.- INTRODUCCIÓN A LA EMPRESA.

2.1.- INTRODUCCIÓN.

La compañía en la cual se ha realizado el plan de seguridad es una empresa de alta tecnología que se constituyó, en el año 2001, con la voluntad de crear un grupo especializado en dirección de proyectos, consultoría de organización y gestión empresarial, que aporta soluciones eficaces para el desarrollo de las empresas y sus proyectos.

Con esto pretende incorporar la experiencia de sus profesionales, al servicio de sus clientes. Es una empresa, que innova, investiga, desarrolla e implanta soluciones en diversos sectores. El equipo de trabajo está compuesto por profesionales con dilatadas trayectorias en el campo de las tecnologías de la información, y amplio conocimiento de los sectores en el que la empresa desarrolla sus soluciones.

2.2.- METODOLOGÍA.

Desarrolla soluciones a medida, tratando a los clientes de forma personalizada, ya que entiende que cada empresa es única y por tanto tiene una problemática distinta. Así, antes de abordar cualquier proyecto se realiza un análisis detallado de las necesidades y particularidades de cada cliente, que unido al conocimiento de sus consultores, permite ofrecerles la solución idónea.
La metodología seguida puede apreciarse en las siguientes premisas desarrolladas por la empresa.

- Relación independiente con el cliente, lo cual permite garantizar una visión objetiva del proyecto a realizar.
- Diseñar propuestas propias y ofertas de servicios, ajustándolas a las necesidades específicas de cada empresa.

- Garantizar el compromiso y dedicación por parte de los profesionales, sin recurrir al empleo de personal con escasa experiencia o ayuda de otras empresas.
- Participar activamente en la motivación de los equipos de trabajo para garantizar la consecución de los objetivos y metas marcados en cada proyecto.
- Contar con acuerdos de colaboración estratégicos con empresas y profesionales de sólida experiencia en distintas áreas.

2.3.- PRODUCTOS Y SERVICIOS.

La empresa se dedica al servicio de distintos sectores, como son los siguientes:

- Sector Sanitario.- Sector complejo, en el que intervienen múltiples factores, desde la administración, los hospitales, los laboratorios farmacéuticos, las compañías de seguros. En todos ellos hay que satisfacer su seguridad y el desarrollo de software necesario para sus aplicaciones.
- Investigación.- Decisiones comerciales basadas en una información incorrecta pueden comprometer la dirección estratégica de la compañía cliente y, finalmente, la supervivencia de la misma. Con este servicio la empresa ayuda a proteger proyectos comerciales, minimiza las pérdidas financieras y preserva datos patentados y corporativos.
- Consultoría Estratégica.- Poner a disposición de sus clientes toda su experiencia a fin de contribuir a realizar una planificación e implantación adecuada de aquellas prácticas y políticas de Recursos Humanos que en cada caso particular puedan ser más adecuadas para una óptima gestión.
- Optimización de procesos.- Determinar los procesos de misión crítica que requieran optimizaciones en las diferentes áreas de la empresa, redefinición e implementación. Los temas que abarca son:

    - Análisis de procesos y las variables que intervienen.
    - Redefinición de procesos.

- Capacitación.
- Puesta en marcha.

2.4.- ORGANIZACIÓN DE LA EMPRESA.

La empresa está dividida en cuatro grandes departamentos, como se puede apreciar en la figura 2.1, dirigidos todos ellos por la dirección general, que tiene todo el poder y se encarga de que todas las demás áreas actúen en armonía y bajo su control.

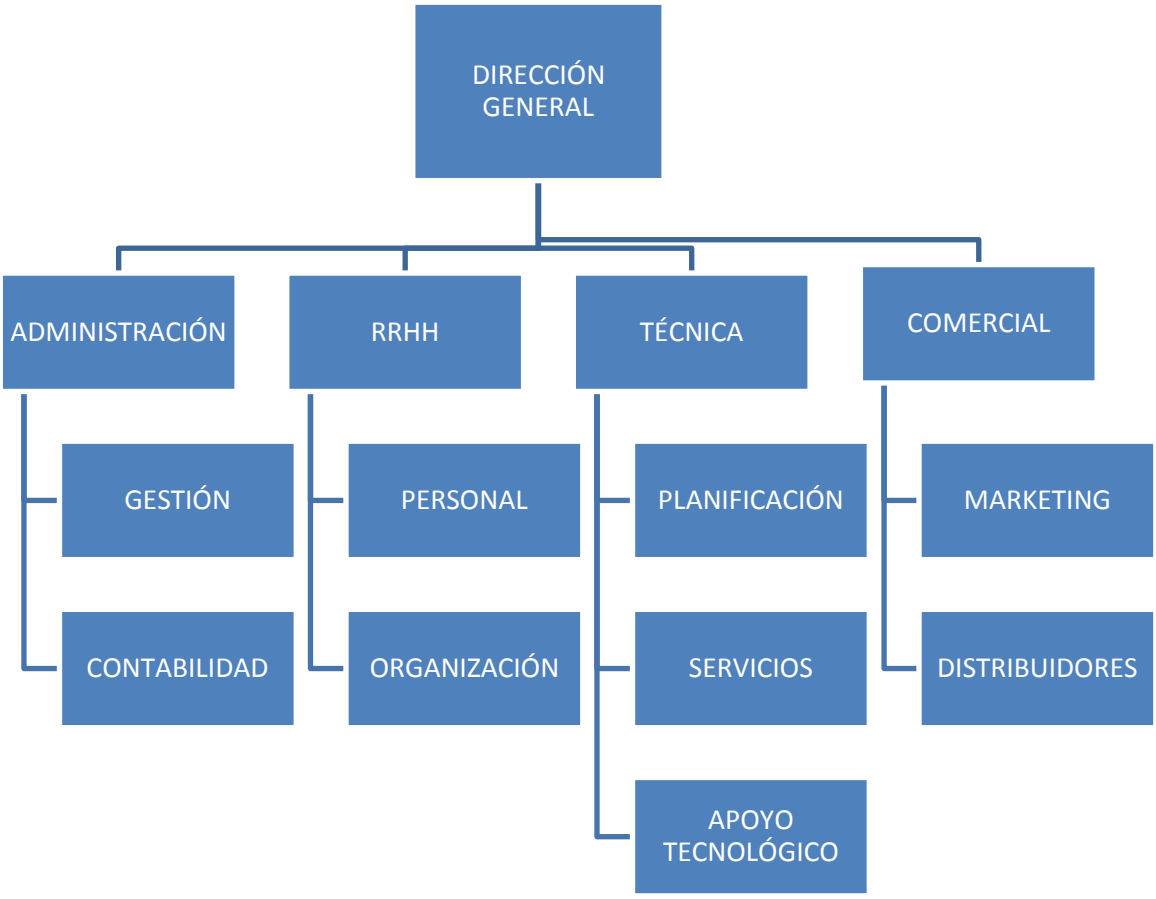

Figura 2.1.- Organigrama de la empresa.

Departamento de Administración.

Este ámbito del organigrama es muy amplio y diverso en funciones y tareas. De hecho se subdivide y separa en:

- Gestión de la Administración.
- Finanzas – Contabilidad.

En cualquier caso, su campo es el de toda la administración de los recursos humanos y materiales, los que al final acaban concretándose en recursos económicos y documentos o justificantes en soportes de papel o informatizado. Incorpora toda la gestión económica y de personal de los demás departamentos. Limitando sus funciones técnicas, comerciales, etc.

Las tareas que realiza el departamento de administración o finanzas son:

- Contabilidad.
- Costes.
- Gestión y previsión de tesorería.
- Cobros y pagos.
- Relación con clientes y proveedores.
- Administración general.
- Elaboración y control de presupuestos.
- Auditoría interna.
- Relaciones laborales.

Departamento de Recursos Humanos.

Gestiona todo lo relativo a la gestión del personal en sentido amplio. Desde captar o recoger las necesidades de contratación de nuevo personal hasta el despido o baja del

mismo, pasando por la gestión de los recursos humanos en forma permanente, todo esto es materia única de esta gerencia.

Las tareas o funciones de este departamento son:

- Selección de personal.
- Contratación de personal.
- Recepción y acogida de nuevos trabajadores.
- Formación del personal.
- Valoración de tareas.
- Sistemas de remuneración del personal: salarios y primas.
- Expedientes del personal.
- Administración de salarios.
- Comunicación interna.
- Relaciones laborales.
- Convenios colectivos.
- Resolución de conflictos laborales.

Departamento Comercial.

Su campo de actuación se dirige hacia la colocación de los servicios, que la empresa ofrece y comercializa a los clientes. Depende, por tanto, de él toda la estructura comercial de la empresa. Integra en su campo las actividades de marketing y de estudio o prospección de mercados. También las de publicidad.

Las funciones de este departamento son:

- La investigación comercial.
- El marketing.
- La planificación comercial.
- Las previsiones de ventas.
- El análisis de los precios.
- Publicidad.
- Gestión de la comercialización.

- Estudio y conocimiento de la competencia.

Este departamento tiene como finalidad última abrir nuevos campos de estudio según se van desarrollando las necesidades del cliente, esto es el caso por ejemplo de investigar los nuevos avances médicos para poder adelantarse a otras empresas en el desarrollo del software.

Departamento Técnico.

Éste es sin duda el departamento más importante de la empresa, puesto que supone todo el desarrollo de negocio de la empresa. Este departamento se encarga de gestionar la actividad a la que la empresa se dedica. Cómo es el desarrollo de software, optimización de procesos de cualquier índole, servicios aplicados a la medicina, etc.

Es por ello que este departamento contiene la mayor parte de la plantilla de la empresa, y consume la mayoría de las instalaciones.

Las funciones que realiza este departamento conforman el grueso de la empresa.

- Proyectos.
- Planificación.
- Oficina técnica.
- Métodos y tiempos.
- Administración de la producción.
- Mantenimiento.
- Control de calidad.
- Los métodos de trabajo.
- El control de calidad de la producción.
- Los servicios de mantenimiento y reparación.
- La investigación e innovación tecnológica.
- El diseño de productos o servicios.

Con este breve análisis del organigrama de la empresa, es necesario para su buen funcionamiento, la coordinación entre ellos, ésta no es posible sin el buen

funcionamiento de toda la red informática y su consiguiente protección de los recursos informáticos.

2.5.- ARQUITECTURA TÉCNICA.

Este punto presenta a nivel general la arquitectura técnica de la compañía y sirve de presentación para las posteriores descripciones de detalle.

La arquitectura de la compañía se fundamenta en los siguientes criterios:

- Centralización de datos y procesos corporativos en un Host, con sistema operativo MVS. Los datos se almacenan en su gran mayoría en un sistema de Base de Datos Relacional DB2, y se explotan generalmente vía Batch o transaccional CICS/ESA, tanto directamente como en aplicativos Cliente/Servidor.
- Modelo de arquitectura Cliente/Servidor, para dotar a los sistemas de información de interfaz más amigable y productiva, así como para descargar al Host de determinados procesos no productivos (validaciones, etc.). Dentro del modelo cliente/servidor, se siguen en la actualidad los criterios:
    1. Presentación en cliente, con los nuevos desarrollos en interfaz gráfica.
    2. Lógica de validaciones formales en cliente.
    3. Lógica de negocio y datos Online contra el Host.
- Comunicaciones APPC directamente contra el Host (Comunicaciones CICS/APPC).
- Impresión operativa descentralizada Online, para documentos de apoyo (proyectos, finiquitos, ofertas, solicitudes, etc.)
- Impresión de documentos contractuales y corporativos centralizadamente, en diferido, para garantizar la calidad de la documentación y la imagen de la compañía (contratos, tarjetas, etc.).

- Informática de agentes con especiales características, para permitirle su trabajo fuera de las sucursales: conexión remota, interfaz GUI, funciones Off-Line....
- Centro de soporte telefónico, los cuales actualmente dan apoyo a los agentes en su labor comercial y centralizan otros servicios (Centro de Ayuda al Usuario (CAU)).

2.6.- ARQUITECTURA HARDWARE.

2.6.1.- TOPOLOGÍA DE RED.

2.6.1.1.- COMPONENTES DE RED.

La red informática de la empresa se compone del siguiente equipamiento:

- 100 PC´s distribuidos entre las 4 sucursales, con aproximadamente 60 de ellos en la casa central.
- 2 Servidores Hewlett Packard, uno para aplicaciones y otro para Internet.
- 4 antenas de transmisión radial.
- 3 enlaces de fibra óptica.
- Cables UTP categoría 5.
- Conexión ADSL con salida a internet.
- Un switch CISCO 4000 en la sede central.
- Soporte para telefonía sobre IP (próximamente las comunicaciones telefónicas internas de la casa central se desarrollarán con este método, usando la línea telefónica solo para las comunicaciones al exterior).
- Conexión al switch central con 64 entradas para PC’s.
- 6 switches CISCO 1900 de 12 entradas, uno en cada en cada sucursal.
- 2 hubs de 100 MB.

2.6.1.2.- DESCRIPCIÓN DE LA RED.

- Enlaces radiales entre sucursales: existe una conexión a través de enlaces radiales que conectan la sede central con el resto de las sucursales, implementado con una topología de tipo BUS. Los datos viajan encriptados mediante un sistema de encriptación propio de las antenas CISCO.
- Fibra óptica entre las conexiones entre las distintas secciones de la empresa.
- UTP en conexiones internas: la totalidad del tendido de cables en el interior de la empresa se realizó con UTP categoría 5.
- Switches: han sido programados para realizar un tipo de encaminamiento: direccionan los paquetes transmitidos por sector, según la dirección IP que traen, distinguiendo a qué sector de la empresa van. De esta manera, al no repetir los paquetes de datos a toda la red, se disminuye el uso de ancho de banda y se evita la divulgación de los mensajes, mejorando la seguridad de la topología de Bus.

En el gráfico topológico de red se puede ver la unión de estos elementos formando la red de la empresa.

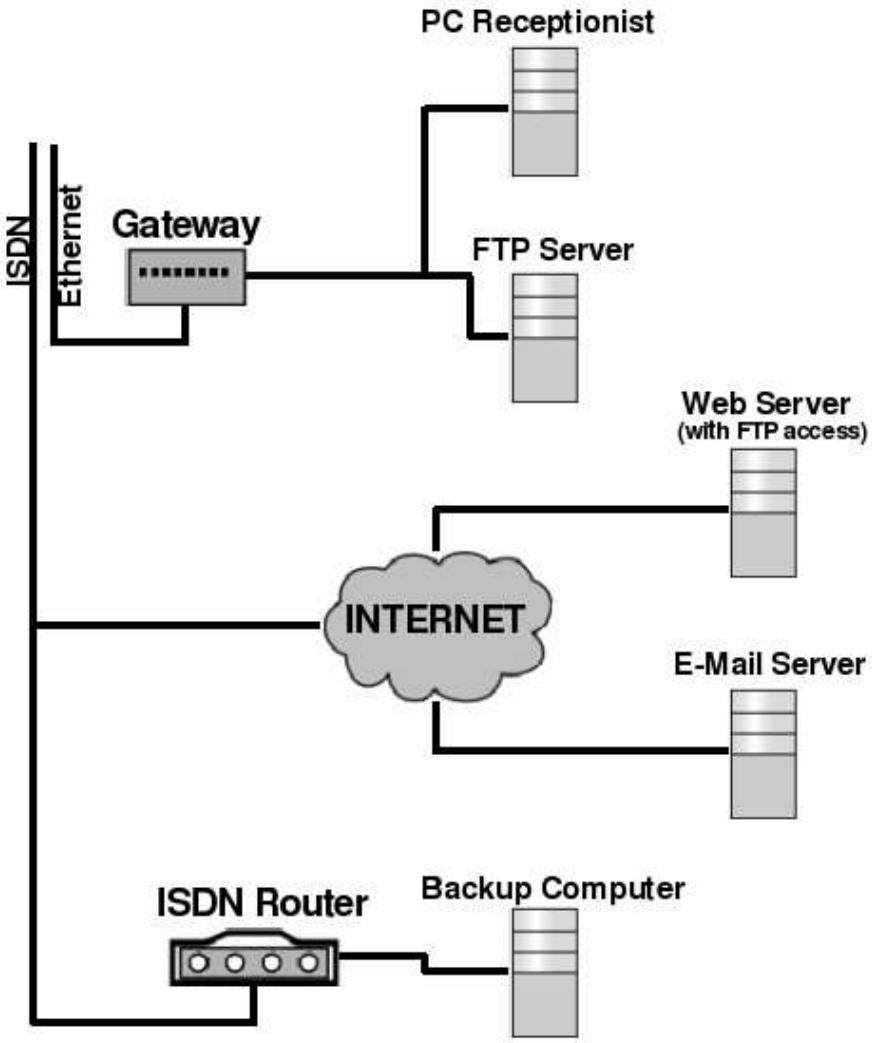

Figura 2.2.- Topología de Red.

2.6.2.- CONEXIONES EXTERNAS.

2.6.2.1.- SEDE CENTRAL.

Dispone de una conexión con aplicaciones propias. Éstas proveen a la empresa de una clave y contraseña de usuario y un proveedor de Internet. La empresa se conecta directamente a la sede a través de la aplicación suministrada, y baja de allí una actualización diaria de archivos necesaria para la gestión. De la misma manera los archivos son transferidos hacia las oficinas.

Las máquinas tienen instalado Internet Explorer con la posibilidad de navegar y los datos que se transmiten acceden por el firewall, pasando directamente a comunicarse al exterior.

2.6.2.2.- SERVIDOR DE INTERNET.

Para la conexión a Internet se utiliza un servidor Proxy de Linux llamado Squid, ubicado en el servidor de Internet. Su salida al exterior es a través de una conexión ASDL, suministrada por un ISP. Este Proxy se configuró de manera estricta, de forma que sólo tiene conexión al exterior un rango de direcciones IP definido por la Dirección. En el servidor Proxy se seleccionaron las direcciones IP de las máquinas que pueden salir al exterior, de esta manera se controla el acceso a Internet. Este Proxy es el que proporciona de acceso a Internet al resto de las sucursales a través de los enlaces radiales.

2.6.2.3.- SERVIDOR DE HOSTING.

El servidor de hosting se eligió según el precio y los servicios ofrecidos. No se ofrece ninguna medida de seguridad ni política de respaldo en caso de problemas, pero no se han registrado problemas hasta el momento.

2.6.3.- EQUIPAMIENTO.

2.6.3.1.- CARACTERÍSTICAS DE LOS SERVIDORES.

En la sede central existen dos servidores iguales con las siguientes características Servidores Hewlett Packard LC 2200, comprados en el año 2002. Uno de ellos es el servidor de aplicaciones y datos, y el otro es servidor de Internet.

Cada uno contiene:

- 2 Procesadores Pentium III 550 MHz.

- 2 Fuentes.
- 2 Placas de red.
- 5 GB de memoria RAM.
- 3 discos con tecnología SCSI con 18 GB de capacidad cada uno.
- Sistema UPS de suministro alternativo de energía.
- Generador de energía eléctrica.

2.6.3.2.- CARACTERÍSTICAS DE LOS PC´S.

La empresa en su totalidad posee alrededor de 100 PC´s, de los cuales 60 están en la sede central. El 40% de estos PC´s son de marca Unisys (60%) o Hewlett Packard (40%). Al ir migrando a aplicaciones y sistemas operativos gráficos, fueron adquiriendo clones con mayor capacidad, actualizando la placa base, el procesador, la cantidad de memoria RAM, y conservando el resto del hardware.

La empresa ha tomado la decisión de asegurar su red, debido al gran costo que implicaba contratar un mantenimiento a terceros permanentemente.

3

ANÁLISIS DE APLICACIONES Y DATOS CRÍTICOS

3.- ANÁLISIS DE APLICACIONES Y DATOS CRÍTICOS.

3.1.- DETERMINACIÓN DE APLICACIONES Y DATOS CRÍTICOS.

Aplicación crítica es toda aquella identificada por su propietario y aprobada por la dirección de la compañía cuya pérdida o falta de disponibilidad ocasiona un efecto catastrófico sobre el desarrollo del negocio.

Son datos críticos todos aquellos que son imprescindibles para el funcionamiento de las aplicaciones consideradas críticas.

Nivel de criticidad.

Para que una aplicación pueda ser considerada como crítica es necesario que su pérdida suponga un impacto profundo y ocasione daños de alguna de las siguientes maneras:

- Cese o reducción importante de los ingresos.
- Imposibilidad de cumplir compromisos con clientes en negocios clave.
- Interrupción importante en el desarrollo y elaboración de productos.
- Retrasos en la elaboración de documentación para clientes o contactos externos considerados como urgentes.
- Gasto de recursos significativos de la compañía para restaurar las aplicaciones.
- Descenso de la cuota de mercado.
- Pérdida de imagen de la entidad.

Las aplicaciones que cumplen estas condiciones son las de nivel de criticidad uno, y dan servicio a las operaciones imprescindibles en la empresa. No pudiéndose prescindir de

ellas en ningún momento, por lo que dichas aplicaciones deben de estar replicadas en al menos dos servidores, por si uno falla el otro pueda prestar el servicio.

Las aplicaciones de nivel de criticidad dos son aquellas cuya no ejecución dificulta la realización de las operaciones pero no llega a paralizar la empresa. En el caso de que ocurra una contingencia que ocasione una parada técnica, la reanudación de las operaciones en el mismo u otro sistema, debe permitir el funcionamiento de al menos las aplicaciones críticas con el nivel de servicio de emergencia que se requiera.

Por último se establecen las aplicaciones con nivel de criticidad tres, la ausencia de estas aplicaciones no condiciona en absoluto los procesos de negocio de la empresa, son aplicaciones que se utilizan en momentos esporádicos del día a día sin afectar al negocio, pudiéndose prescindir de ellas en cualquier momento.

GRADO DE CRITICIDAD	CONDICIONES	TIEMPO DE ATENCIÓN
1	Los procesos no pueden continuar	Inmediato
2	Los procesos pueden continuar, pero con dificultad	Inmediato
3	Los procesos continúan sin problemas	10 minutos

Tabla 3.1.- Grados de criticidad.

La identificación de las aplicaciones críticas se ha llevado a cabo mediante la distribución y recogida de cuestionarios entre los jefes de proyecto de la dirección de sistemas de información, analizando con posterioridad la información recibida. Los resultados del análisis se han contrastado con la dirección de organización.

3.2.- APLICACIONES CRÍTICAS PARA LA EMPRESA

Dentro de la empresa se pueden diferenciar distintos tipos de aplicaciones, dependiendo de la información que contienen y las personas que tienen acceso a dicha información. Es por esto que hay que tener especial cuidado en el resguardo de los datos y el acceso al personal de la empresa, como se detallará más adelante.

Los tipos de aplicaciones que se pueden encontrar dentro de la empresa son:

- Aplicaciones desarrolladas por la empresa: son aquellas que realiza la empresa o contienen información relevante de la lógica de negocio.
- Aplicaciones internas de la empresa: estas aplicaciones contendrían información de la empresa.
- Aplicaciones de uso normal para el personal de la empresa.

Una vez visto el tipo de criticidad que existe y los distintos tipos de aplicaciones que hay en la empresa, se puede establecer la relación que hay entre ambas.

Figura 3.1.- Aplicaciones Críticas.

4

SEGURIDAD FÍSICA Y LÓGICA DE LA INFORMACIÓN

4.- SEGURIDAD FÍSICA Y LÓGICA DE LA INFORMACIÓN DE LA EMPRESA.

4.1.- SEGURIDAD FÍSICA.

Los edificios o inmuebles propiedad de la compañía disponen de diversos sistemas de seguridad para garantizar la integridad y la confidencialidad de los bienes y documentos que tiene la empresa en su haber. A continuación se detallan los sistemas de protección que posee actualmente la entidad:

4.1.1.- SEGURIDAD FÍSICA DE LOS EDIFICIOS.

Sistemas de extinción de incendios.

En caso de incendio, su extinción puede realizarse con medios manuales o automáticos. Los medios manuales se basan en extintores portátiles, mangueras, etc. Es importante resaltar que el elemento extintor localizado en un área es el apropiado para el previsible tipo de incendio a declararse en ella.

Los medios automáticos se basan en la inundación del área mediante agua, ya que es el más recomendable por su bajo coste y su nulo impacto en el entorno.

Este mecanismo tiene un mecanismo de reacción que, en caso de llegar a un estado de alerta o de alarma, sustituye el aire de la conducción por agua. La actuación de estos sistemas de extinción debe estar combinada con la previa desconexión del suministro de energía eléctrica del área afectada.

Sistemas de alarmas.

- Alarmas mediante infrarrojos: El sistema avisa al centro de control cuando se detecta un movimiento en alguna habitación mientras el sistema esté activado.
- Alarmas mediante vibración: El sistema avisa al centro de control cuando se detecta el intento o violación de alguna puerta de la empresa. Este sistema se encuentra instalado en algunas puertas clave de la empresa, como pueden ser, la puerta de acceso principal, puertas de acceso secundarias y puerta de acceso a la sala central donde se alojan los servidores de almacenamiento con todos los datos de los procesos de negocio de la compañía.

Para el control y administración de estas detecciones se emplean paneles computarizados, controlados por medio de una clave personal que al introducirla, activa o desactiva el sistema de seguridad. Una vez activada, este panel de control se alimentará de la información que le envíen los distintos tipos de sensores instalados, los que, al ser vulnerados, activarán un ruido acústico y junto con ello se reportará la información al centro de control mediante la línea telefónica.

Acondicionamiento del aire.

Se debe tener en cuenta que los recursos informáticos, especialmente los de las grandes instalaciones de la empresa, generan calor, esto hace necesario un acondicionamiento del aire para disipar dicho calor, manteniéndose así el ambiente con la temperatura y la humedad adecuadas dentro de los límites indicados por los fabricantes.

La suficiente potencia de estos equipos permitirá que trabajen desahogadamente y que las operaciones de mantenimiento sean sencillas y frecuentes. Un elemento fundamental del sistema acondicionador que posee, es el mecanismo de corte automático tras producirse una detección de incendio.

4.1.2.- CONTROLES DE ACCESO.

Estos controles pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con accesos permitidos) y para resguardar la información confidencial de accesos no autorizados.

Las personas que no desarrollen su actividad profesional dentro de la empresa y quieran acceder a ella por diversos motivos (negocios, reuniones, visitas, entrevistas, etc.) deberán presentar su documento nacional de identidad o en caso de no estar en posesión del mismo, su pasaporte o documento similar, este documento será mostrado al vigilante de seguridad de la entrada, el cual, almacenará en una base de datos los siguientes datos:

- Nombre.
- Apellidos.
- Fecha de nacimiento.
- Número de documento.

Todo este almacenamiento se hará de acuerdo a la ley orgánica de protección de datos 15/1999 (LOPD).

4.2.- SEGURIDAD LÓGICA.

Necesaria para proteger los activos de información de la empresa para que sean siempre utilizados de forma autorizada, y sólo por razones de negocio, y evitar acciones que puedan provocar su alteración, borrado o divulgación no autorizados, de forma accidental o intencionada.

Los objetivos que se intentan cubrir son:

- 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.
- Que la información transmitida sea recibida solo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

4.2.1.- SEGURIDAD EN EL ACCESO A LA INFORMACIÓN.

Es la primera línea de defensa para la mayoría de los sistemas computerizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

A continuación se detalla el reglamento que cumplen las diferentes partes implicadas en garantizar la seguridad de la información de la empresa.

Identificación de usuarios.

Es la clave que permite a un usuario acceder de forma individual a un sistema de información.

Cada identificador de usuario está asignado a una persona, que es responsable de las actividades realizadas por él.

El identificador de usuario se asigna a una persona para facilitarle el acceso a un único sistema de información, y adquiere otros identificadores para el uso de otros sistemas. En la empresa para evitar esta multiplicidad se define y utiliza una nomenclatura estándar en la creación de identificadores, de forma que un usuario tenga el mismo identificador en todos los sistemas que necesite utilizar.

Con este sistema de identificación se consigue:

- Utilizar un método de Identificación única, que permita al usuario realizar los procesos de identificación y autenticación una sola vez, en la primera conexión al sistema.
- Dedicar un sistema a las funciones de control de seguridad, de modo que antes de permitir el acceso del usuario a cualquier sistema de información, se verifique una sola vez su identidad y autorizaciones de acceso. Este Sistema es gestionado por el administrador de seguridad.

Autorización de Usuarios.

El acceso de cada usuario a los sistemas de la empresa tiene que ser aprobado previamente por la dirección. Hay definido un procedimiento, manual, para autorizar la inclusión de nuevos identificadores de usuarios en el sistema y que incluya la notificación al director responsable del usuario.

Eliminación de Usuarios.

En caso de terminación de la necesidad de uso por razones de negocio o abandono de la empresa, hay definido un procedimiento, manual, para la eliminación de identificadores de usuarios del sistema. El director del usuario es responsable de comunicar a la administración de seguridad las condiciones de que son motivo dicha eliminación.

El procedimiento incluye los controles para prevenir el acceso de un usuario a los sistemas, inmediatamente después de la comunicación de su director. Un identificador de usuario eliminado, no se volverá a asignar a ninguna otra persona en el futuro.

Control de contraseñas.

- El acceso a la información sensible de la compañía, aplicaciones y sistemas informáticos está regulada contra accesos no autorizados, requiriéndose, dentro del ámbito informático el uso de una clave de usuario y una contraseña para poder acceder a ella.
- La contraseña elegida por el usuario será cambiada regularmente, en torno a una vez cada tres meses.
- La contraseña no podrá ser vista en ningún momento y en ningún sistema.
- El número de intentos de escritura de la contraseña estará limitado a tres intentos, bloqueándose el terminal en caso de superar dicho límite.
- La contraseña deberá ser una combinación de números y letras no relacionadas con ningún dato de carácter personal.
- Las contraseñas se almacenan en una base de datos encriptada a la que será imposible su acceso, ni siquiera para lectura simple.
- La contraseña debe tener una longitud mínima de 6 caracteres, o tener al menos un carácter numérico y uno alfabético.
    - No empezar ni terminar con un número, no tener más de tres caracteres consecutivos idénticos, en cualquier posición, a los de una contraseña usada anteriormente.
    - No tener más de dos caracteres iguales consecutivos.

- Ser cambiada, al menos, cada 60 días para usuarios generales y cada 30 días para usuarios que tengan algún tipo de privilegio o autoridad. Tiene que haber instalado un control que informe a los usuarios cuando su contraseña tenga que ser cambiada.
- No ser reutilizada hasta después de, al menos, 12 cambios.
- No contener el identificador de usuario, como parte de la contraseña.

- Un sistema automático rechazará las contraseñas que no cumplan la normativa.
- El personal relacionado con la seguridad dispondrá de procedimientos de recuperación de contraseñas para los casos en los que a los usuarios se les haya olvidado.

Restauración de contraseñas.

Hay definido e implantado un proceso para asegurar la restauración o cambio de contraseña, por pérdida u olvido de la anterior o cuando se sospeche que es conocida por otra persona.

El proceso incluye la identificación positiva del solicitante o, en caso contrario, el envío de la nueva contraseña al director del usuario. Este proceso es automatizado para favorecer la gestión de la contraseña por el propio usuario o su director inmediato. Tanto la solicitud como la respuesta se realizan a través de un medio seguro.

Control del sistema.

- El personal de seguridad y los responsables de la información, revisarán semestralmente los privilegios de acceso de los empleados, para así asegurarse de que solo se aplican a aquellos usuarios que debido a sus responsabilidades les han sido asignados, y los procedimientos definidos, para asegurarse de manera inmediata, preferiblemente automática, de cortar el acceso a las aplicaciones a aquellos usuarios que hayan sido cesados en sus privilegios o que no están en activo.

- Existen procedimientos definidos para dar de baja en los sistemas informáticos a los usuarios.
- El acceso a la información estará restringido a tipos específicos de requerimientos de uso.
- Los empleados de la empresa siempre que quieran acceder a una aplicación, lo harán activando una transacción, debiendo identificar al principio de la ejecución.
- El acceso al mantenimiento de la red de comunicaciones y a los puertos de los números telefónicos estará reservado a personal específicamente autorizado, debiendo existir un método de encriptación o cualquier método alternativo de protección, apropiado a las necesidades del negocio, a la sensibilidad de los sistemas de información y a los datos.

Protección en terminales.

- Todo usuario es responsable de proteger el terminal que le ha sido asignado, y colaborar en la protección de cualquier otro terminal de la empresa, para evitar que sea robado o dañado.
- Se congelarán automáticamente las aplicaciones, se limpiarán las pantallas de contenido y se bloqueará el uso de estaciones de trabajo, para evitar acciones de personas no autorizadas, si no hay actividad en ellas, durante un periodo superior a treinta minutos, requiriéndose la entrada de una nueva contraseña para poder desbloquear la estación de trabajo.
- Los procedimientos de conexión presentarán información de seguimiento del mismo, en la pantalla de la estación de trabajo, indicando los pasos y el proceso de log-on.
- Las diversas aplicaciones presentarán pantallas de aviso poniendo de manifiesto la realización de accesos no autorizados, mostrando mensajes como que el sistema está restringido única y exclusivamente a usuarios con autorización, tomándose medidas legales en caso de violar estas reglas.
- Cuando los terminales requieran compartir accesos, por razones de negocio, los procedimientos deberían asegurar que solo las personas con autorización puedan acceder.

- Las estaciones de trabajo no se deben dejar sin atención mientras se realice el proceso de Log-on (Ejemplo: Accesos a ficheros exclusivos del terminal) a menos que exista una seguridad física o lógica.
- Al finalizar la jornada laboral, se utilizarán los mecanismos de bloqueo lógicos.

Control de las comunicaciones.

- Autorizaciones de acceso:
  - La autorización de acceso tiene que ser verificada mediante un identificador de usuario y contraseña válidos. Una vez verificada la identidad del usuario que está accediendo, no debe haber restricciones para establecer la conexión, salvo las propias de la sesión o servicio con el que vaya a trabajar.
  - Hay definidos y establecidos controles para detectar y manejar los ataques sistemáticos contra el gateway. Su propietario es informado cada vez que el número de accesos no autorizados sobrepase un límite previamente establecido en la instalación.
- Conexiones desde el exterior.
  - Cualquier acceso, por razones de negocio de la empresa, a los sistemas o servicios internos a través de un gateway, es justificado por el usuario, aprobado por la dirección y registrado en la relación de autorizaciones del gateway, a través del cual se vaya a acceder. Todo ello, antes de ser establecida la conexión, esto facilita a un usuario trabajar desde un terminal portátil o desde su propio domicilio.
- Conexiones hacia el exterior.
  - El gateway puede ser usado para el acceso a sistemas o servicios ajenos a la empresa, desde terminales controlados por ella. La utilización de este sistema facilita a un usuario la utilización, desde su puesto de trabajo, de redes, sistemas y servicios ajenos a la empresa, que cada vez son más necesarios.
- Sistema Firewall (Cortafuegos).

- Este sistema protege las comunicaciones entre un usuario y una red externa, de la forma más transparente posible para el usuario, facilitándole al máximo los servicios que dicha red ofrece.
- El sistema firewall implantado en la empresa está diseñado para asegurar el tráfico con internet, debido a que representa la mayor fuente de información y de medios de comunicación con terceros, incluyendo: clientes, suministradores y cualquier otro tipo de personas que comparten intereses comunes.

- Correo Electrónico.

  Además de las consideraciones generales de seguridad a aplicar en cualquier sistema de uso público, hay que tener en cuenta:

  - La posibilidad de interceptación de mensajes o notas, por lo que no debe incluirse en ellos información sensible que no esté cifrada.
  - La posible inclusión de virus o código dañino en los activos de información recibidos.

4.2.2.- SEGURIDAD EN LAS ESTACIONES DE TRABAJO.

Control de los datos.

- Los datos deben tener una copia de seguridad (backup) en un medio apropiado y con una frecuencia definida por el propietario.
- Las copias de seguridad serán almacenadas en un lugar alejado del centro de procesos de la compañía.
- Las estaciones de trabajo que trabajen con aplicaciones críticas del negocio deberán ser incluidas en el plan de recuperación.
- Se debe realizar una limpieza de los posibles virus de acuerdo a un determinado periodo que podrá ser una vez a la semana.
- Toda la información y todos los programas descargados de la red deberán estar sujetos al mismo nivel de seguridad y controles que la información de la entidad.

- Habrá que prestar mucha atención cuando en los ordenadores portátiles haya información que pueda ser vista por personas sin autorización.
- La información que contenga un código ejecutable deberá ser siempre supervisada con un antivirus antes de ser ejecutada.
- Para garantizar la máxima seguridad, las estaciones de trabajo deben de tener un antivirus que se ejecutase cada vez que ésta se enciende y una persona se identifica.

Control del software.

- Cada copia original de cada producto de software deberá estar guardada en un lugar seguro.
- Se debe realizar algunas copias del sistema operativo para propósitos de backup.
- Toda estación de trabajo deberá tener su sistema operativo, instalado a partir de software legal y original, con su número de licencia etiquetado en la parte frontal de la CPU del terminal, cumpliendo así con la legislación vigente.
- Las condiciones de licencia del software deberán ser supervisadas cada cierto tiempo.
- La adquisición de software ilegal no deberá ser realizada bajo ningún concepto.
- Toda la adquisición de software deberá ser chequeada con un antivirus antes de usarse.
- Discos compactos vírgenes deberán ser revisados mediante un antivirus antes de iniciar su uso.
- Cualquier medio de almacenamiento, sea del tipo que sea, debe de ser supervisado por un antivirus.
- El material sensible de los usuarios deberá estar guardado en un cajón bajo llave a ser posible.

4.2.3 INTEGRIDAD DE LA INFORMACIÓN.

Asignación de recursos y activos.

El objetivo es definir un método de clasificación de los activos de información de la empresa, para su protección frente a pérdida, divulgación no autorizada o cualquier otra forma de uso indebido, ya sea de modo accidental o intencionado.

La información adopta muchas formas, tanto en los sistemas como fuera de ellos. Puede ser:

- Almacenada, en los sistemas o en medios portables.
- Transmitida, a través de redes o entre sistemas.
- Impresa o escrita, en papel y o hablada, en conversaciones.

Bajo el punto de vista de seguridad, la protección adecuada debe ser aplicada a todas y cada una de las formas relacionadas con un sistema de información, es decir, a la tratada por medios informáticos.

Protección de la información clasificada.

La principal regla de protección es que la información clasificada sea conocida o utilizada, sólo por personas autorizadas y siempre por razones del negocio de la empresa.

Todos los empleados tienen que tener suscrita con la empresa, o ser requeridos para ello, una cláusula de confidencialidad en la que firmen el compromiso de protección y no divulgación de la información clasificada que manejen por motivos de trabajo. De esta manera la información clasificada de la empresa queda guardada en cualquier sistema o medio de almacenamiento puesto que posee los medios físicos y lógicos adecuados para protegerla, no permite su acceso público y limita el acceso a esta información.

5

POLÍTICA DE RESPALDO DE LA INFORMACIÓN

5.- POLÍTICA DE RESPALDO DE LA INFORMACIÓN.

5.1.- COPIAS DE SEGURIDAD (BACKUP).

Uno de los elementos en los que se tienen que centrar las recomendaciones de protección de un plan de contingencia es la información. Una empresa debe tener bien elaborada una política de copias de seguridad.

De entre todas las interrupciones a las que se puede ver expuesta, en muchas de ellas será necesario recuperar información y es en ese punto en el que si no se tiene una buena planificación de copias de seguridad, la situación en la que se verá la empresa después de recuperar los datos puede que no sea la más idónea para la continuidad de la operaciones.

Un plan de contingencia contemplará una política de backup, es decir, dirá qué hay que guardar, cuándo y dónde hay que guardarlo, dónde hay que almacenar las copias y de cara a una eventual recuperación de datos, cómo llevar a cabo la restauración de los mismos.

Dicho esto, la principal finalidad de las copias de seguridad es la de mantener la continuidad del negocio de la empresa ante cualquier pérdida de datos en el menor tiempo posible y con la máxima exactitud.

REQUISITOS QUE DEBEN CUMPLIR.

Poseer la información planificada.

Cuando se planifica una política de backup, no siempre se guarda lo mismo (se verá más adelante). Simplemente este requisito a lo que obliga es a tener la información planificada, en el soporte previsto. Si se está haciendo una copia de las bases de datos de

clientes, no pueden aparecer ficheros de proveedores ya que después de una restauración la situación no sería la correcta.

Tener una mínima probabilidad de error.

Para cumplir este requisito hay que tener en cuenta dos factores. Por un lado, la integridad de los datos guardados, ya que hacer una copia de seguridad de datos corruptos no sirve de nada. Y por otro lado utilizar soportes de almacenamiento en buen estado. Estar en un lugar seguro y bajo acceso autorizado.

Es conveniente que el soporte o soportes utilizados para la copia estén desconectados del sistema del cual se han sacado los datos e inmediatamente sean guardados en un lugar seguro. Cuando se habla de lugar seguro se refiere a un lugar con acceso restringido y protegido de ciertos peligros como incendios o inundaciones. Y por supuesto para completar esta seguridad no se puede olvidar proteger los soportes con la pestaña que impide que puedan ser borrados.

Rápida y eficiente recuperación de la información.

Una vez hecho un backup, hay que tener la seguridad de que ante una posible necesidad de recuperar la información que almacena, se va a poder realizar en el menor tiempo posible la restauración de todos los datos previstos.

TIPOS DE COPIAS DE SEGURIDAD.

Los tipos de copias de seguridad se pueden clasificar en dos tipos:

- Copias de todo lo que hay en el origen.
- Copias de todo lo modificado.

Copias de todo lo que hay en el origen.

También llamadas copias completas. Son muy simples en lo referente a que copian todo lo que se encuentra en el origen y lo almacenan en el destino. Como destino se pueden

elegir diferentes tipos de soportes, los cuales se verán más adelante. Algo que hay que tener en cuenta cuando se realizan este tipo de copias es que suelen ocupar mucho espacio y normalmente es necesario invertir bastante tiempo para realizarlas.

Por otro lado, este tipo de copias permiten restaurar un sistema fácilmente ante una catástrofe. Cuando se dice que copian todo, ese todo es literal: no es una seguridad que almacena todos los ficheros o todas las carpetas. Las copias completas guardan desde el sistema operativo de la máquina o la estructura de directorios, hasta los perfiles de usuario, estructuras de datos y toda aquella información necesaria si se restaura la copia en una máquina que no sea la de origen, para que se pueda funcionar exactamente de la misma manera que en el momento en que se hizo la seguridad.

Cuando se realiza una copia de este tipo, se borra todo lo que tenían los soportes de almacenamiento antes, es decir, se vacía el catálogo. Para realizar la copia podrá usarse o bien un software de copias de seguridad o bien algún mandato u opción proporcionada por el propio sistema operativo. En función de la alternativa empleada, podrá ser necesario inicializar los soportes antes de empezar la copia. Esto que puede parecer tan obvio, es importante que sea tenido en cuenta sobre todo por las personas encargadas de realizar las copias. Como se ha dicho, una copia completa puede durar mucho tiempo y puede que sea necesario usar varios soportes.

Las copias en la empresa se realizarán como mínimo cuando se va a llevar a cabo alguna acción que ponga en peligro la integridad y mantenimiento de la información. Como puedan ser durante cortes prolongados de luz, cambios de máquina o si se habla de PC de usuario antes de despedir a algún trabajador o de cara a revisiones de contrato o negociaciones de sueldo.

Lo recomendable es realizar una copia de este tipo de forma periódica, de todas las máquinas consideradas críticas y en horarios de mínima actividad.

Copias de todo lo modificado.

Dentro de las copias de todo lo modificado, se pueden distinguir dos tipos:

- Copias incrementales.
- Copias diferenciales.

Copias incrementales.

También llamadas copias de archivos modificados o copias evolutivas. Cada vez que se hace una copia de este tipo, no se guardan todos los archivos, sino sólo aquellos que han sido modificados.

Copias diferenciales.

Al igual que en las copias incrementales, en las diferenciales no se guardan todos los archivos, sino sólo aquellos que han sido modificados.

Las copias diferenciales examinan fechas de creación y modificación. Se guarda todo aquello que haya sido creado o modificado desde la última copia de seguridad completa. La política de respaldo de la información de la empresa ha buscado una secuencia óptima de copias en la que se entremezclen copias completas, increméntales y diferenciales.

Periodicidad y tipo de la extracción de copias:

Las copias de respaldo se deben realizar diariamente para todos los ficheros de la empresa de forma duplicada en dos servidores distintos de respaldo. Asimismo se conservarán copias semanales y mensuales de todos los ficheros que surjan cambios. El encargado de dichas operaciones es el administrador del sistema.

Elemento respaldado / Servidor Respaldado	Servidor Primario		Servidor Secundario	
Sistema Operativo	S	C	S	C
Software Básico	M	C	M	C
Software de Aplicaciones	S	I	S	D
Bloques y Tablas de Control	D	D	D	I
Bases de Datos	D	I	D	D
Sistema Integro	S	C	S	C

Tabla 5.1.- Periodicidad y Tipo de copia.

Periodicidad:	Tipo de copia
D= Diaria.	C=Completa.
S= Semanal.	I=Incremental.
M= Mensual.	D=Diferencial.

Secuencia de respaldo utilizada en la empresa durante dos semanas:

LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES	SÁBADO	DOMINGO
Diferencial /Incremental	Diferencial /Incremental	Diferencial /Incremental	Diferencial /Incremental	Completo	Diferencial /Incremental	Diferencial /Incremental
LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES	SÁBADO	DOMINGO
Diferencial /Incremental	Diferencial /Incremental	Diferencial /Incremental	Diferencial /Incremental	Completo	Diferencial /Incremental	Diferencial /Incremental

Tabla 5.2.- Secuencia de Respaldo.

Esta secuencia de respaldo es una de las más utilizadas y consiste en Respaldos completos cada semana y respaldos increméntales o diferenciales cada día de la semana.

Con este sistema la empresa se asegura tener la información correcta después de un posible fallo del sistema.

Por ejemplo, si la empresa sufre un fallo el jueves de la segunda semana, será necesario el respaldo completo realizado el viernes junto con el respaldo diferencial del miércoles en el caso de haber utilizado estos.

5.2.- SOPORTE DE ALMACENAMIENTO.

Existen numerosos tipos de soportes de almacenamiento en el mercado. La decisión de elegir unos u otros depende principalmente del volumen de información que maneje la empresa, en este caso cintas, ya que para poder grabar datos en un soporte físico más o menos perdurable se usan casi en exclusiva las tecnologías óptica y magnética.

Sin embargo esta decisión ha estado también condicionada por un conjunto de variables, tales como:

- La frecuencia de realización de las copias.
- El volumen de datos a copiar.
- La disponibilidad de la copia.
- El tiempo de recuperación del sistema.

El tipo de cintas utilizadas por la empresa son de la familia DLT ofreciendo 110 Gb de almacenamiento y 11 Mbps de tasa de transferencia además de compatibilidad opcional con otros productos de la familia en caso de necesitar un refuerzo en la seguridad.

Elemento respaldado	**Soporte Físico**
Sistema Operativo	C
Software Básico	D
Software de Aplicaciones	D
Bloques y Tablas de Control	C
Bases de Datos	C
Sistema Integro	C

Tabla 5.3.- Soporte físico.

D= DVD/RW.

C= Cintas Magneto/óptico.

5.3.- GUARDADO DE LA INFORMACIÓN.

El dónde guardar los soportes que almacenan la información de los backup que se realizan es otro de los puntos importantes en una planificación de copias de seguridad. Y es que no vale cualquier sitio, cuando la información con la que se está jugando es la que puede hacer que desaparezca una organización ante un desastre. Por ello la empresa dispone de una sala con armarios ignífugos, protegida de ciertos peligros como incendios o inundaciones en la que se dispone de un juego de copias.

Además la empresa dispone de otra sala con las mismas medidas en otras instalaciones en las que se trabaja para prevenir la seguridad de la información ante una posible catástrofe .

Elemento respaldado	**Lugar de Almacenamiento**
Sistema Operativo	C
Software Básico	B
Software de Aplicaciones	B
Bloques y Tablas de Control	A
Bases de Datos	C
Sistema Integro	C

Tabla 5.4.- Lugar de almacenamiento.

A= En otro local.

B= En la propia oficina.

C= En ambos.

Ahora se observará en la siguiente tabla el número de copias que se realizan de los datos de la empresa así como del número de versiones que disponen de cada elemento.

Elemento respaldado	Número de Copias	Numero de Versiones
Sistema Operativo	2	2
Software Básico	1	1
Software de Aplicaciones	2	1
Bloques y Tablas de Control	2	2
Bases de Datos	2	3
Sistema Integro	2	3

Tabla 5.5.- Número de copias y versiones activas.

5.4.- ACCESO A LA INFORMACIÓN.

Para completar las medidas de seguridad que se han de tomar a la hora de guardar los soportes de almacenamiento es bueno recordar que no sólo vale con tener las copias en lugares seguros, también se debe proteger la información y no sólo la de los backup, sino toda, de personal no autorizado.

Los backup los ha de guardar el personal indicado a tal efecto. Ellos son los encargados de seguir las pautas indicadas en la planificación y los responsables ante cualquier fallo. El acceso a cualquier copia debe estar autorizado por el responsable de seguridad y no por cualquier persona por muy alto directivo que pueda ser.

Pueden parecer reglas muy estrictas, pero se dan circunstancias en las que ciertas copias están en poder de personal ajeno al grupo de seguridad u ocasiones en las que personal de desarrollo solicita datos o restauraciones.

En la medida de lo posible hay que evitar esta situación, ya no por la maldad o el desconocimiento de la gente, sino por mantener el máximo control e intentar adaptarse a lo establecido en el plan de contingencia y documento de seguridad.

5.5.- RESTAURACIÓN DE DATOS.

La restauración de los datos es el fin por el que hay que luchar a la hora de realizar una buena planificación de copias de seguridad. Esta es por tanto la última etapa a la hora de recuperar los datos perdidos de la empresa.

Los casos más típicos son dos:

- Restaurar ficheros o carpetas sueltas.
- Restaurar el sistema desde cero.

Para hacer frente al primer caso se debe saber si el fichero, carpeta, biblioteca... ha sido creado o modificado desde la última copia completa. En caso afirmativo habrá que usar la copia incremental o diferencial más reciente. Si por el contrario es información que no ha sido modificada desde la última copia completa o si se necesita restaurar información de un día concreto, se echará mano o bien de la última copia completa o bien de la copia completa más cercana a la fecha solicitada.

Para resolver el segundo caso se deberá echar mano de la última copia completa que tenga la empresa y después de las copias increméntales o diferenciales realizadas desde entonces. Restaurando la copia completa estará generando un sistema con el mismo sistema operativo, misma estructura de directorios... y con las copias de archivos modificados se estarán dejando los datos lo más actualizados posible.

6

RIESGOS Y MEDIDAS PREVENTIVAS

6.- RIESGOS Y MEDIDAS PREVENTIVAS.

6.1- ANÁLISIS DE RIESGOS.

El análisis de riesgos que se ha efectuado ha permitido investigar los riesgos a los que están expuestos los sistemas de información y recomendar las medidas apropiadas que deberán adaptarse para controlar dichos riesgos. Permite evaluar el impacto que podría resultar de la pérdida de la confidencialidad, integridad o disponibilidad de los sistemas de información. Una vez realizado el análisis de riesgos se procede a implantar las medidas de protección necesarias para paliar las posibles catástrofes que conllevarían las ocurrencias de las posibles amenazas a las que está expuesta la empresa. Este método proporciona a los responsables de la organización informática, la información adecuada sobre la que basar sus decisiones.

A continuación se explicarán los conceptos relacionados con el análisis a realizar, para una mejor comprensión.

RIESGO.

Riesgo se puede definir como una medida del grado de exposición al que un sistema, y por tanto una organización está sujeta. El riesgo es una función de:

- La probabilidad de la ocurrencia o manifestación de una amenaza.
- El grado de vulnerabilidad del sistema que pueda ser aprovechado por una amenaza para causar un impacto no deseado.
- El nivel de afecto adverso que la ocurrencia de la amenaza tendría en la organización.

En lo relacionado con la tecnología, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición de una pérdida. (por ejemplo el riesgo de perder datos debido a una rotura de disco, virus informáticos, etc.)

La Organización Internacional por la Normalización (ISO) define riesgo tecnológico como:

> "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de una activo o un grupo de activos, generándole pérdidas o daños".

En la definición anterior se pueden identificar varios elementos que se deben comprender adecuadamente para comprender el concepto de riesgo.

Estos elementos son: amenazas, vulnerabilidades, activos e impactos.

A continuación se analizan cada uno de ellos:

AMENAZA.

Un evento, persona o idea que presenta un peligro para un sistema. La ocurrencia o manifestación de una amenaza puede comprometer la confidencialidad, integridad o disponibilidad de un activo integrante de la empresa, utilizando las vulnerabilidades del mismo pueden ser de carácter físico o lógico, como ser una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo.

ACTIVO.

Componente del sistema al que la organización asigna un valor y que por tanto necesita protección. Su valor puede quedar muy reducido después de la ocurrencia de una amenaza. Los activos pueden ser tangibles como por ejemplo, el personal, edificios, hardware, software, datos, documentación, etc. O pueden ser intangibles como la imagen, la reputación de la empresa, confianza de los clientes, etc.

VULNERABILIDAD.

Debilidad de un sistema a través del cual una amenaza pueda actuar. La vulnerabilidad suele ser debida a la ausencia de medidas de protección, al mal funcionamiento de las

mismas o la cobertura parcial que dichas medidas proporcionan frente a la amenaza. La presencia de una vulnerabilidad en sí, no causa daño, debe de existir una amenaza para aprovecharse de ella. Si tal amenaza no existe, la vulnerabilidad no requiere la implantación de un sistema de protección.

Estas vulnerabilidades son de naturaleza variada. A modo de ejemplo se citan las siguientes: falta de conocimiento del usuario, tecnología inadecuada, transmisión por redes públicas, etc. Una vulnerabilidad común es contar con un antivirus no actualizado, la cual permitiría al virus actuar y ocasionar daños.

IMPACTO.

La consecuencia indeseable de la ocurrencia de una amenaza que afecta a los activos del sistema y resulta una pérdida para la organización. El impacto podría ser uno o más de los siguientes:

- Indisponibilidad o destrucción de los activos.
- Modificación no autorizada del software o de los datos.
- Revelación no autorizada de datos o de software.
- Pérdida de confianza y reducción de la eficiencia.
- Pérdida de oportunidades de negocio.
- Pérdida de vidas humanas.
- Afectación del medio ambiente.

SALVAGUARDA.

La salvaguarda es una medida de protección que mejora la seguridad del sistema y protege los activos de las amenazas mediante:

- La transferencia del riesgo.
- La reducción de la probabilidad de manifestación de una amenaza.

- La reducción del nivel de vulnerabilidad del que podría aprovecharse una amenaza.
- La reducción del impacto de la manifestación de una amenaza.
- La detección de la manifestación de una amenaza.
- La recuperación del impacto de la manifestación de una amenaza.

Hay que distinguir dos aspectos importantes:

1.- Servicio de salvaguarda: acción que reduce el riesgo.
2.- Mecanismo de salvaguarda: procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

La siguiente figura muestra los elementos y sus interrelaciones.

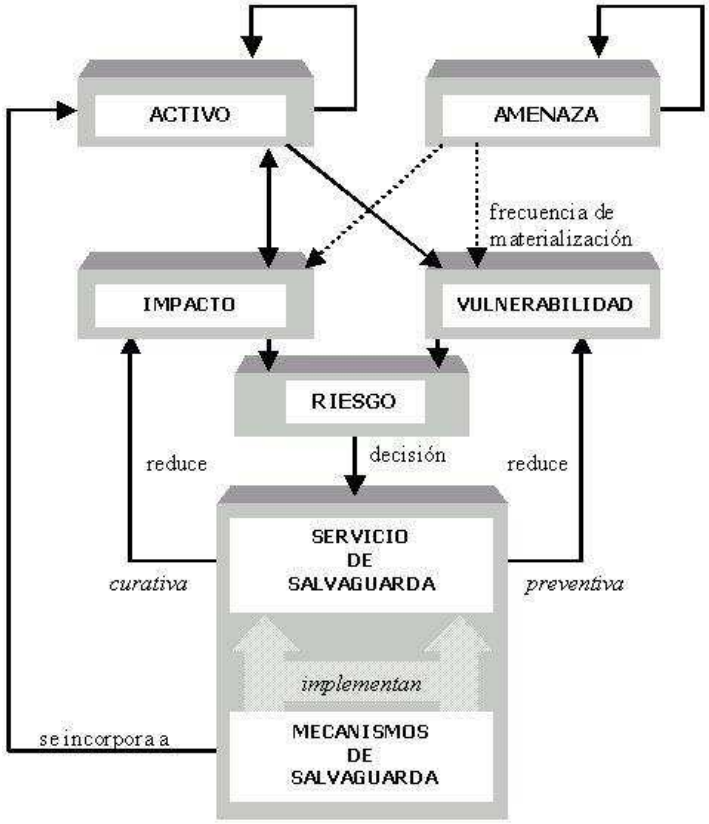

Figura 6.1.- Componentes de riesgo.

6.2.- IDENTIFICACIÓN DE LOS RIESGOS.

Para determinar los riesgos o las posibles amenazas a las que está expuesta la empresa, éstos se han dividido en tres grupos: riesgos naturales, riesgos inducidos y riesgos informáticos.

- Riesgos naturales:
    - Incendio.
    - Tormenta.
    - Inundaciones.
    - Terremoto.
- Riesgos de fallos en los suministros:
    - Corte de la electricidad.
    - Corte sistema de refrigeración.
    - Corte de agua.
    - Corte de las telecomunicaciones.
- Riesgos inducidos:
    - Sabotaje.
    - Atentado terrorista.
    - Amenaza de bomba.
    - Vandalismo.
    - Huelga.
- Riesgos informáticos:
    - Riesgos errores humanos:
        - Error de desarrollo.

- Error de soporte técnico.
- Error de explotación.
- Error de usuario.
- Robo o pérdida de equipos.
- Robo o pérdida de documentación.
- Ausencia de personas clave.
- Mal uso del correo electrónico.

- Riesgos de fallos en los equipos:

  - Fallo de hardware.
  - Ataques de virus.

Los principales riesgos a los que están expuestas las empresas según las estadísticas son:

CONTINGENCIA	PORCENTAJE
TERRORISMO	25 %
HURACANES Y TERREMOTOS	17 %
INCENDIOS	17 %
CORTES DE CORRIENTE	9 %
ERRORES DE SOFTWARE	9 %
INUNDACIONES	7 %
PERFORACIÓN DE TUBERÍAS	5 %
ERRORES DE HARDWARE	4 %
CORTES DE COMUNICACIÓN	4 %
OTROS FACTORES	3 %

Tabla 6.- Principales riesgos.

6.3.- SISTEMA DE VALORACIÓN DE RIESGOS

El sistema de valoración de riesgos utilizado adopta un modelo que permite clasificarlos atendiendo a tres factores:

1. Impacto que produciría el desastre en la empresa:

   - Total: (valor tipo T = 3) este nivel se dará cuando no se pueda disponer del lugar físico por un periodo superior al máximo tolerado para la interrupción , de las prestaciones mínimas o el tiempo que demoran las tareas de restablecimiento de todas o algunas de las prestaciones sea mayor al periodo máximo aceptable.
   - Parcial: (valor tipo P = 2)en el caso en que los equipos han sufrido daños menores que permiten el funcionamiento parcial de los sistemas, o sus prestaciones pueden ser realizadas por otros equipos. Es necesaria la acción de alguien externo (proveedores, mantenimiento, etc.).
   - Menor: (valor tipo M = 1) en el caso en que los desperfectos de solucionan mediante la preinstalación y/o reconfiguración de los equipos, y por lo tanto no es necesaria la acción de alguien externo para superar la situación de emergencia.

2. Probabilidad de ocurrencia del desastre:

   - Alta: Cuando la tasa de aparición del desastre es alta (probable = 3)
   - Media: Cuando la tasa de aparición del desastre es media (posible = 2)
   - Baja: Cuando la tasa de aparición del desastre es baja (remoto = 1)

3. Gravedad de continuidad / ocurrencia (peso):

- peso 1 = incidencia menor (afecta poco)

  .....

  peso 10 = incidencia grave (afecta mucho)

Para sacar el valor total del peso que tiene el riesgo para la empresa se utiliza una ecuación en la que intervienen los tres factores anteriormente indicados.

Ecuación:

$$peso\ total = \frac{\text{tipo} * \text{peso}}{\text{probabilidad}}$$

6.4.- VALORACIÓN DE RIESGOS.

6.4.1.- VALORACIÓN DE RIESGOS NATURALES.

RIESGO DE INCENDIO.

DEFINICIÓN.

El incendio es un fuego que generalmente suele tener un tamaño significativo aunque éste también puede ser pequeño. La posibilidad de que surja un incendio en la compañía es una amenaza muy crítica y un riesgo al que siempre se está expuesto. La aparición de esta amenaza puede conllevar a la destrucción de diversos activos muy importantes para la entidad, como pueden ser el hardware y software o incluso, la documentación en posesión de la empresa, que sería mucho más catastrófico.
Si el incendio toma un carácter más fuerte, el riesgo de destrucción de los activos podría migrar a ser un riesgo contra la integridad física del personal de la empresa, llegando a una situación máxima alerta.

CAUSAS.

Las causas por las que se puede producir un incendio son las siguientes:

- Producirse un cortocircuito en algún punto de la red eléctrica.
- Generación de alguna chispa o sobrecalentamiento de algún material orgánico (madera, fibra, corcho, etc.).
- Fallo en las calderas de la calefacción
- Cigarros mal apagados cerca de algún material inflamable.
- Incendio provocado por algún sujeto.
- Sobrecalentamiento de algún aparato eléctrico.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo un incendio son las siguientes:

A) Incendio del edificio.

- Destrucción completa del edificio.
- Destrucción de todos o de la mayor parte de los terminales.
- Destrucción completa o de la mayor parte de la información de la empresa.
- Destrucción de los servidores.
- Destrucción de las copias de respaldo.
- Destrucción de las aplicaciones de software.
- Lesiones o bajas en el personal de la empresa.
- Paralización total a largo plazo de los procesos de negocio.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Muy alta, 10.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**10**	**30**

Tabla 6.1.- Valoración de Incendio en todo el edificio.

B) Incendio en una parte del edificio.

- Destrucción parcial del edificio.
- Destrucción de una parte de los terminales.
- Destrucción parcial de la información de la empresa.
- Posible destrucción de los servidores.
- Posible destrucción de las copias de respaldo.

- Posible destrucción de algunas aplicaciones de software.
- Posibles lesiones del personal de la empresa.
- Paralización total a corto plazo de los procesos de negocio.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 5.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**6**	**12**

Tabla 6.2.- Valoración de Incendio en parte del edificio.

C) Incendio localizado en alguna sala de la compañía.

- Daños en algunos terminales.
- Destrucción de documentación almacenada en papel.
- Posible daño de los servidores (caso de que el fuego se localice en la sala de servidores).
- Posible lesión leve de algún empleado de la entidad.
- Pérdida de alguna aplicación de software.
- Posible pérdida de alguna copia de respaldo que no se encontrara en el armario.
- Posible parada leve de algún proceso de negocio.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 3.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**1**	**4**	**4**

Tabla 6.3.- Valoración de Incendio en alguna sala.

RIESGO DE TORMENTA.

DEFINICIÓN.

Una tormenta es un fenómeno atmosférico caracterizado por la coexistencia próxima de dos o más masas de aire de diferentes temperaturas.

El contraste térmico y otras propiedades de las masas de aire (humedad) dan origen al desarrollo de fuertes movimientos ascendentes y descendentes, produciendo una serie de efectos característicos, como fuertes lluvias y viento en la superficie e intenso aparato eléctrico

CAUSAS.

Las tormentas que se producen por las nubes que se desarrollan cuando la atmósfera está inestable. Se entiende por atmósfera inestable aquella situación en la que se producen importantes movimientos del aire en sentido vertical. Esto ocurre cuando el aire es más frío de lo habitual en la parte más alta de la troposfera, lo que suele ocurrir cuando pasa un frente frío o bien en situaciones de bajas presiones.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo una tormenta son las siguientes:

A) Impacto de un rayo en el edificio.

- Posible destrucción parcial del edificio.

- Daños en los servidores.
- Daños en diversos terminales cercanos al impacto del rayo.
- Posibilidad de producirse algún incendio.
- Lesión de algún empleado de la empresa.
- Pérdida de información, si ésta estaba cercana al impacto del rayo.
- Posible parada de los procesos de negocio de la empresa.
- Corte del suministro de electricidad.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media/Alta, 7.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**7**	**21**

Tabla 6.4.- Valoración de Impacto de un rayo en el edificio.

B) Corte de electricidad de larga duración debido a la tormenta.

- Paralización de los servicios informáticos.
- Paralización de la actividad empresarial.
- Paralización de cualquier proceso de negocio.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 4.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**4**	**12**

Tabla 6.5.- Valoración de corte de electricidad de larga duración.

C) Corte de electricidad de corta duración.

- Leve paralización de los servicios informáticos.
- Leve paralización de la actividad empresarial.
- Leve paralización de cualquier proceso de negocio.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**2**	**2**	**2**

Tabla 6.6.- Valoración de corte de electricidad de corta duración.

RIESGO DE INUNDACIONES.

DEFINICIÓN.

Una inundación es la ocupación por parte del agua de zonas que habitualmente están libres de ésta. Es uno de los desastres naturales que más pueden dañar a los sistemas de información de la empresa.

CAUSAS.

Las causas que producen las inundaciones son las siguientes:

- Desbordamiento de los ríos.
- Precipitaciones muy intensas de agua.
- Rotura de cañerías.
- Negligencias al manipular el agua.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo las inundaciones son las siguientes:

A) Inundaciones con serios daños a la estructura del edificio.

- La estructura del edificio no garantiza la seguridad de mantenerse en pie.
- Se paralizan las actividades empresariales durante un largo periodo de tiempo.
- Serios daños en los sistemas de información de la empresa.
- Posibles pérdidas de las copias de respaldo.
- Posible inutilización de los servidores.
- Posibles lesiones leves del personal.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Muy Alta, 10.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**10**	**30**

Tabla 6.7.- Valoración de Inundación en el edificio.

B) Inundaciones sin daños a la estructura del edificio.

- Posible paralización de los procesos de negocio durante un corto periodo de tiempo.
- Daños en algunos terminales.
- Daños en cierta documentación empresarial.
- Posibilidad de daños en los servidores.
- Posibilidad de daños en las copias de respaldo.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media / Alta, 7.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**7**	**21**

Tabla 6.8.- Valoración de Inundación sin daño en el edificio.

C) Filtraciones de agua o humedades en alguna sala de la compañía.

- Paralización de las actividades que se estén llevando a cabo en la sala donde se ha producido la incidencia.
- Posibles daños de algún terminal que se encontrara cerca de la filtración.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	2	2	2	2

Tabla 6.9.- Valoración de Filtraciones o humedades.

RIESGO DE TERREMOTO.

DEFINICIÓN.

Se denomina sismo, seísmo o terremoto a las sacudidas o movimientos bruscos del terreno generalmente producidos por disturbios tectónicos o volcánicos.

CAUSAS.

El origen de la gran mayoría de los terremotos se encuentra en una liberación de energía producto de la actividad volcánica o a la tectónica de placas.
A pesar de que la tectónica de placas y la actividad volcánica son la principal causa por la que se producen los terremotos, existen otros muchos factores que pueden dar lugar a temblores de tierra:

- Desprendimientos de rocas en las laderas de las montañas.
- Hundimiento de cavernas.
- Variaciones bruscas en la presión atmosférica por ciclones.
- La propia actividad humana.

Estos mecanismos generan eventos de baja magnitud que generalmente caen en el rango de microsismos, temblores que solo pueden ser detectados por sismógrafos.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo los seísmos son las siguientes:

A) Seísmo de gran magnitud.

- Posible destrucción parcial o total del edificio.
- Serios daños en la estructura del edificio.
- Destrucción de la información de la empresa.
- Importantes daños en diversos terminales.
- Posible pérdida de las copias de respaldo.
- Lesiones e incluso bajas del personal.
- Posible pérdida de los servidores.
- Paralización total por un largo periodo de tiempo de los procesos de negocio.
- Destrucción de las aplicaciones de software.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Muy Alta, 10.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**10**	**30**

Tabla 6.10.- Valoración de Seísmo de gran magnitud.

B) Seísmo de menor magnitud.

- Posibles daños en la estructura del edificio.
- Destrucción parcial de la información de la empresa.
- Importantes daños en ciertos terminales.
- Posibles daños en las copias de respaldo.
- Lesiones del personal de la empresa.
- Daños en la sala de servidores.
- Pérdida de ciertas aplicaciones de software.

- Paralización por un periodo de tiempo considerable de la actividad empresarial.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 6.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**6**	**18**

Tabla 6.11.- Valoración de Seísmo de menor magnitud.

C) Temblores sin consecuencias graves.

- El edificio no sufre daños estructurales.
- Pequeña pérdida de información.
- Posibles daños puntuales en algún terminal.
- Posibles daños puntuales en las copias de respaldo.
- Posibles lesiones leves del personal de la empresa.
- Posibles daños puntuales en los servidores.
- Paralización momentánea de la actividad empresarial.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 3.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	2	1	3	6

Tabla 6.12.- Valoración de Temblores sin consecuencias.

6.4.2.- VALORACIÓN DE RIESGOS EN EL SUMINISTRO.

RIESGO DE CORTE DE ELECTRICIDAD.

DEFINICIÓN.

Un corte de electricidad se refiere a aquellas veces cuando el servicio eléctrico regular se ha interrumpido por daño en las líneas de transmisión. La compañía eléctrica suministradora no es capaz de hacer llegar electricidad a la compañía. Durante una situación de desastre, la energía eléctrica puede estar interrumpida durante días o semanas.

CAUSAS

Las causas por las que se puede producir un corte de electricidad son las siguientes:

- Por causas naturales:
  - Fuego, terremoto, inundaciones, tormenta, hielo, etc.
- Por otras causas:
  - Fallo en las centrales eléctricas.
  - Sobrecarga en la red.
  - Conexión de algún aparato que supere la potencia máxima.
  - Impago de la cuota mensual.
  - Corte del suministro eléctrico inducido.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo un corte de electricidad son las siguientes:

A) Corte del suministro eléctrico por un largo periodo de tiempo.

- Paralización total de la actividad empresarial.
- Pérdida de la última información creada o modificada que no hubiese sido guardada.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media/Alta, 7.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**7**	**21**

Tabla 6.13.- Valoración de Corte eléctrico por un largo periodo.

B) Corte del suministro eléctrico por un corto periodo de tiempo.

- Paralización total de la actividad empresarial por un tiempo menor que el anterior.
- Pérdida de la última información creada o modificada que no hubiese sido guardada.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media/Baja, 4.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**4**	**8**

Tabla 6.14.- Valoración de Corte eléctrico por un corto periodo.

C) Corte momentáneo del suministro eléctrico.

- Paralización total de la actividad empresarial por un periodo de tiempo muy corto.
- Pérdida de la última información creada o modificada que no hubiese sido guardada.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Media/Baja, 4.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**2**	**4**	**2**

Tabla 6.15.- Valoración de Corte momentáneo de electricidad.

RIESGO DE CORTE DE SUMINISTRO DE AGUA.

DEFINICIÓN.

Paralización del suministro de agua hacia la empresa debido algún motivo. La empresa carece de abastecimiento de agua en sus instalaciones.

CAUSAS.

Las causas que pueden producir un corte en el suministro de agua son las siguientes:

- Rotura de tuberías.
- Impago de la cuota mensual.
- Averías en la compañía suministradora.
- Averías cercanas al edificio de la empresa.
- Averías interiores del edificio.
- Corte por largos periodos de sequía.
- Cortes inducidos.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo un corte de agua son las siguientes:

A) Cortes de agua por periodos superiores a un día.

- Posible parada de los servidores por recalentamiento.
- Posible paralización de los procesos de negocio.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media / Baja, 4.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**4**	**8**

Tabla 6.16.- Valoración de Cortes de Agua superiores a un día.

B) Cortes de agua por periodos inferiores a un día.

- Posible parada de los servidores por recalentamiento.

- Posible paralización de los procesos de negocio.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**1**	**2**	**2**

Tabla 6.17.- Valoración de Cortes de Agua inferiores a un día.

C) Cortes esporádicos de agua.

- Paralización espontánea de los procesos de negocio sin incidencias graves.
- Posible parada leve de los servidores.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**2**	**2**	**1**

Tabla 6.18.- Valoración de Cortes esporádicos de agua.

RIESGO DE CORTE DE LAS TELECOMUNICACIONES.

DEFINICIÓN.

Paralización del sistema de comunicaciones de la empresa, las conexiones telefónicas con el exterior y el interior de la compañía no funcionan.

CAUSAS.

Las causas que pueden producir un corte en las telecomunicaciones son las siguientes:

- Avería o fallo de la compañía suministradora.
- Corte inducido de las telecomunicaciones.
- Cortes debidos a desastres naturales como por ejemplo el fuego, terremoto, inundaciones, tormenta, hielo, etc.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo un corte en el sistema de telecomunicaciones de la compañía son las siguientes:

A) Corte de las telecomunicaciones por un largo periodo de tiempo.

- Paralización de los procesos de negocio que se apoyen en la línea telefónica para subsistir.
- Imposibilidad de atender a los clientes durante varios días.
- Imposibilidad de conexión con las sucursales.
- Imposibilidad de acceso a varias aplicaciones informáticas por tiempo indeterminado.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 5.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**5**	**10**

Tabla 6.19.- Valoración de Cortes de telecomunicaciones.

B) Corte de las telecomunicaciones por un corto periodo de tiempo.

- Paralización de los procesos de negocio que se apoyen en la línea telefónica para subsistir por tiempo menor a un día.
- Imposibilidad de atender a los clientes por tiempo menor a un día.
- Imposibilidad de conexión con las sucursales y las agencias.
- Imposibilidad de acceso a varias aplicaciones informáticas por tiempo menor a un día.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 2.

Gravedad de la ocurrencia: Baja, 3.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**2**	**3**	**3**

Tabla 6.20.- Valoración de Cortes de telecomunicaciones por un periodo corto.

C) Parada momentánea de las telecomunicaciones.

- Paralización de los procesos de negocio que se apoyen en la línea telefónica para subsistir por tiempo muy breve.

- Imposibilidad de atender a los clientes durante un periodo muy breve de tiempo.
- Imposibilidad de conexión con las sucursales y las agencias en ciertos momentos muy breves.
- Imposibilidad de acceso a ciertas aplicaciones informáticas por un periodo momentáneo.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**2**	**2**	**1**

Tabla 6.21.- Valoración de parada momentánea de las telecomunicaciones.

6.4.3.- EVALUACIÓN DE RIESGOS INDUCIDOS.

RIESGO DE SABOTAJE.

DEFINICIÓN.

El sabotaje es una acción deliberada dirigida a debilitar la compañía mediante la subversión, la obstrucción, la interrupción o la destrucción de material. El sabotaje es utilizado como una forma de reivindicación organizada por los trabajadores para impactar negativamente en la empresa, apuntando a un objetivo común.

CAUSAS.

Las causas que pueden producir un sabotaje son las siguientes:

- Descontento de los empleados con la compañía
- Abuso desmesurado de la empresa hacia el personal
- Impago de los salarios por parte de la compañía
- Despidos masivos sin justificación
- Incumplimiento de las leyes por parte de la empresa
- Promesas realizadas por la empresa sin cumplirlas a posterior

CONSECUENCIAS.

Las consecuencias que pueden traer consigo el sabotaje son las siguientes:

A) Sabotaje con importantes daños en los activos empresariales.

- Serios daños en la estructura del edificio.
- Paralización total de los procesos de negocio por un largo periodo de tiempo.
- Pérdida de información de la compañía.
- Posible pérdida de las copias de respaldo.
- Serios daños en las estaciones de trabajo.
- Posibles daños en la sala de servidores.
- Cortes de distintos suministros.
- Destrucción de aplicaciones de software.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Alta, 9.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**9**	**27**

Tabla 6.22.- Valoración de Sabotaje con importantes daños.

B) Sabotaje con diversos daños en los activos empresariales.

- Daños puntuales sin graves consecuencias en la estructura del edificio.
- Paralización de la actividad empresarial por un corto periodo de tiempo.
- Pérdida de información de la empresa.
- Posible pérdida de las copias de respaldo.
- Daños puntuales en los terminales.
- Posibilidad de daños en los servidores.
- Posibilidad de cortes de suministro.
- Posibilidad de destrucción de aplicaciones de software.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 6.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**6**	**18**

Tabla 6.23.- Valoración de Sabotaje con diversos daños.

C) Sabotaje con daños leves o muy leves en los activos empresariales.

- Parada de la actividad que se estuviera realizando en el lugar donde se produce el sabotaje.
- Posibles pérdidas puntuales de la información de la compañía.
- Pequeños daños en algún terminal.
- Posibilidad de cortes de suministro.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	2	1	2	4

Tabla 6.24.- Valoración de Sabotaje con daños leves.

RIESGO DE ATENTADO TERRORISTA.

DEFINICIÓN.

Acción mediante la cual se busca dañar la integridad física o moral de una o varias personas, mediante la utilización de la violencia, armas o artefactos explosivos. Es una acción que también puede estar dirigida a distintos inmuebles. En la compañía se valora el riesgo del edificio en sufrir un ataque terrorista.

CAUSAS.

Las causas que pueden llevar a cabo un atentado terrorista son las siguientes:

- Situaciones de presión política.
- Situaciones de presión ante los jueces.
- Sembrar el caos y el miedo.
- Respuesta a acciones de un estado no compartidas por el terrorismo.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo un atentado terrorista son las siguientes:

A) Atentado con un impacto gravísimo en el edificio de la compañía.

- Posible caída parcial o total del edificio.
- Serios daños en la estructura del inmueble.
- Destrucción de la información de la empresa.

- Destrucción de la mayoría de los terminales.
- Pérdida de los servidores.
- Destrucción de las copias de respaldo.
- Pérdidas de capital humano y lesiones muy graves.
- Destrucción de las aplicaciones de software.
- Paralización de la actividad empresarial por un largo periodo de tiempo.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Muy Alta, 10.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**10**	**30**

Tabla 6.25.- Valoración de Atentado con impacto grave.

B) Atentado con serio impacto en el edificio de la compañía.

- Posible caída parcial del edificio.
- Daños en la estructura del inmueble.
- Pérdida de una parte de la información de la entidad.
- Serios daños en ciertos terminales.
- Posible pérdida de los servidores.
- Posible destrucción de las copias de respaldo.
- Posibles pérdidas de capital humano y lesiones graves y leves.
- Posible pérdida de ciertas aplicaciones de software.
- Paralización de la actividad empresarial por un tiempo considerable.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Alta, 8.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	3	1	8	24

Tabla 6.26.- Valoración de Atentado con impacto serio.

C) Atentado con daños leves en el edificio de la compañía.

- Posibles daños leves en la estructura del edificio.
- Posible pérdida de una pequeña parte de la información de la entidad.
- Daños leves en ciertos terminales.
- Lesiones leves del personal.
- Paralización de la actividad empresarial por un corto periodo de tiempo.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 3.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	2	1	2	4

Tabla 6.27.- Valoración de Atentado con daños leves.

RIESGO DE AMENAZA DE BOMBA.

DEFINICIÓN.

Situación mediante la cual se formula el anuncio de una posible explosión de un artefacto explosivo en el edificio de la compañía o en las inmediaciones cercanas a la sede de la entidad, poniéndose en peligro la vida de diferentes personas y también los activos empresariales.

CAUSAS.

Las causas de una amenaza de bomba son muy parecidas a las del riesgo anterior y son las siguientes:

- Situaciones de presión política.
- Avisos falsos de personas.
- Situaciones de presión ante los jueces.
- Sembrar el caos y el miedo.
- Respuesta a acciones de un estado no compartidas por el terrorismo.
- Pequeño artefacto colocado por algún empleado descontento.

CONSECUENCIAS.

Las consecuencias para este escenario dependerán de la gravedad del impacto de la bomba en el edificio, por lo que habría que volver al riesgo de atentado terrorista para evaluarlo, aunque por regla general se pueden incluir las siguientes consecuencias:

A) Amenaza de bomba con explosión de la misma.

- Daños en la estructura del inmueble.
- Desalojo del edificio.
- Pérdida de una parte de la información de la entidad.
- Daños en ciertos terminales.
- Posibles pérdidas de capital humano y lesiones graves y leves.
- Paralización de la actividad empresarial por un tiempo considerable.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Alta, 8.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**8**	**24**

Tabla 6.28.- Valoración de Amenaza de bomba con explosión.

B) Amenaza veraz de bomba.

- Desalojo del edificio.
- Paralización de la actividad empresarial por un tiempo no muy largo (1 día).
- Daños parecidos al escenario A en caso de explosión de la bomba.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 5.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**5**	**10**

Tabla 6.29.- Valoración de Amenaza veraz de bomba.

C) Falsa amenaza de bomba.

- Desalojo del edificio.
- Paralización de los procesos de negocio por un corto periodo de tiempo.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	1	1	2	2

Tabla 6.30.- Valoración de Falsa amenaza de bomba.

RIESGO DE VANDALISMO.

DEFINICIÓN.

Situación mediante la cual los ciudadanos por motivos, los cuales, pueden ser muy diferentes en cada caso, buscan dañar diversos bienes materiales sean de la naturaleza que sean, como señal de protesta aunque a veces no tiene porque ser así. Este riesgo puede ser muy peligroso cuando se produzca en las inmediaciones de la empresa, ya que la misma estaría expuesta a la pérdida de diversos activos empresariales.

CAUSAS.

Las causas que pueden producir una situación de vandalismo son las siguientes:

- Revueltas políticas.
- Revueltas estudiantiles.
- Revueltas laborales.
- Celebraciones de fiestas.
- Celebraciones deportivas.
- Terrorismo callejero.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo una situación de vandalismo son las siguientes:

A) Vandalismo con graves consecuencias con el personal fuera o dentro del edificio.

- Lesiones del personal.
- Daños en diversos terminales.
- Pérdida de información de la compañía.
- Posible daño en las copias de respaldo.
- Posible daño a los servidores.
- Paralización de los procesos de negocio por un tiempo considerable.
- Desalojo del edificio.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 6.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**6**	**12**

Tabla 6.31.- Valoración de Vandalismo con graves consecuencias.

B) Vandalismo leve con el personal dentro del edificio.

- Paralización de la actividad empresarial por un corto periodo de tiempo.
- Desalojo del edificio.
- Posibles lesiones leves del personal.
- Posibles daños leves en los terminales.
- Posible pérdida puntual de información.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 3.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**3**	**6**

Tabla 6.32.- Valoración de Vandalismo con leves consecuencias.

C) Vandalismo leve con el personal fuera del edificio.

- Leves daños en los componentes del edificio.
- Posibles daños leves en los terminales.
- Posible pérdida puntual de información.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**1**	**2**	**2**

Tabla 6.33.- Valoración de Vandalismo con personal en el exterior.

RIESGO DE HUELGA.

DEFINICIÓN.

Una huelga es una acción emprendida de forma individual o por un colectivo social consistente en dejar de hacer una cosa o cosas, dentro de las funciones del colectivo o individuo, para una presión social, con vistas a la obtención de un objetivo concreto. La huelga laboral es una acción colectiva, emprendida por un grupo de trabajadores, consistente en negarse a cumplir total o parcialmente el trabajo que le es encomendado.

Normalmente se emplea como medio de ejercer presión en las negociaciones con el empresario, para obtener una mejora en las condiciones laborales, aunque ocasionalmente se utiliza como represalia con otros fines. Internacionalmente la huelga es reconocida como un derecho fundamental de los trabajadores.

CAUSAS.

Las causas que pueden producir una huelga son las siguientes:

- Descontento del personal hacia la compañía.
- Incumplimiento de la empresa de las normas o leyes hacia los trabajadores.
- Reivindicaciones sobre las condiciones laborales que el trabajador considera insuficientes.
- Huelga general convocada por los sindicatos.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo una huelga son las siguientes:

A) Huelga con un largo periodo de duración y sin servicios mínimos.

- Paralización total de los procesos de negocio de la entidad.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 6.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**6**	**18**

Tabla 6.34.- Valoración de Huelga de larga duración.

B) Huelga con un corto periodo de duración y con servicios mínimos.

- Paralización parcial de los procesos de negocio de la empresa.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 3.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**3**	**6**

Tabla 6.35.- Valoración de Huelga de corta duración.

C) Huelga general con carácter vigente de un día.

- Paralización por un día de la actividad empresarial.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Muy Baja, 1.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	1	1	1	1

Tabla 6.36.- Valoración de Huelga de un día de duración.

6.4.4.-EVALUACIÓN DE LOS RIESGOS INFORMATICOS.

Los riesgos informáticos se van a dividir en dos grupos por un lado los errores que pueda cometer el personal de la empresa y por el otro lado los posibles fallos que puedan surgir en los diferentes equipos, a continuación se pasa a detallar cada grupo.

6.4.4.1.- RIESGOS PRODUCIDOS POR ERRORES HUMANOS.

RIESGO DE ERROR DE DESARROLLO.

DEFINICIÓN.

Errores que se producen a la hora del desarrollo de una determinada aplicación o a la hora de la instalación de la misma, son errores introducidos por el personal de la empresa, generalmente de manera negligente e ignorando las consecuencias que pueden tener, aunque también se puede dar el caso de introducir estos errores teniendo constancia de los mismos.

CAUSAS.

Las causas que pueden producir este tipo de errores son las siguientes:

- Errores humanos sin intención de hacer daño.
- Errores humanos con intención de hacer daño.

- Intrusión de virus.
- Desconocimiento de la tecnología por parte de programador.
- Desconocimiento de la tecnología por parte del analista.
- Falta de experiencia de las empresas de desarrollo de aplicaciones.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo un error de desarrollo son las siguientes:

A) Errores que afecten seriamente al proceso de negocio.

- Parada de la actividad a la que afecte el error.
- Posible pérdida de confidencialidad, integridad o disponibilidad de la información.
- Incapacidad de la aplicación de cubrir todas las necesidades del proceso de negocio.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media/Baja, 4.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**4**	**12**

Tabla 6.37.- Valoración de Errores que afecten seriamente.

B) Errores que afecten levemente al proceso de negocio.

- Parada momentánea de la actividad a la que afecte el error.
- Baja probabilidad de pérdida de confidencialidad, integridad o disponibilidad de la información.

- Incapacidad de la aplicación de cubrir alguna de las necesidades del proceso de negocio.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**2**	**2**	**2**

Tabla 6.38.- Valoración de Errores que afecten levemente.

C) Errores sin relevancia.

- El proceso de negocio puede continuar sin problemas.
- Son errores que no afectan a la confidencialidad, integridad y disponibilidad de la información.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Alta, 3.

Gravedad de la ocurrencia: Baja, 0.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**3**	**0**	**0**

Tabla 6.39.- Valoración de Errores sin relevancia.

RIESGO DE MANTENIMIENTO.

DEFINICIÓN.

Situación en la que se producen distintos errores de mantenimiento, tanto de software como de hardware por parte del equipo de mantenimiento de la compañía.

CAUSAS.

Las causas que pueden producir un error en el mantenimiento de los sistemas de información son las siguientes:

- Falta de piezas de sustitución en el almacén.
- Errores en el pronóstico y diagnóstico de las averías.
- Falta de preparación por parte del equipo de mantenimiento.
- Errores en la adaptación a la empresa de nuevas aplicaciones.
- Errores en la actualización del software de la empresa.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo un error de mantenimiento son las siguientes:

A) Errores de mantenimiento que afecten a los servidores.

- Paralización de los procesos de negocio.
- Posible pérdida de información empresarial.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 3.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**3**	**6**

Tabla 6.40.- Valoración de Errores de mantenimiento en los servidores.

B) Errores de mantenimiento que afecten a los terminales.

- Paralización del trabajo que se esté llevando a cabo en el terminal o terminales afectados.
- Si afecta a varios terminales, paralización parcial de la actividad que se lleva a cabo en esos terminales.
- Posible pequeña pérdida de información.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Baja, 1.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**2**	**1**	**0.5**

Tabla 6.41.- Valoración de Errores de mantenimiento en los terminales.

C) Errores de mantenimiento que afecten a las aplicaciones.

- Paralización del uso de la aplicación afectada por el personal de la compañía.
- Paralización del proceso de negocio que utilice dicha aplicación.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	1	1	2	2

Tabla 6.42.- Valoración de Errores de mantenimiento en las aplicaciones.

RIESGO DE ERROR DE USUARIO.

DEFINICIÓN.

Errores introducidos en los sistemas de información de la empresa, por parte de lo usuarios que pueden ser debidos a diferentes causas. Estos errores pueden ser por ejemplo:

- Introducción incorrecta varias veces de la contraseña de usuario para acceder al terminal.
- Introducción incorrecta de datos personales de los clientes, errores introducidos en los contratos con clientes y empleados, etc.

CAUSAS.

Las causas que pueden producir un error de usuario son las siguientes:

- Desconocimiento por parte del usuario de los procedimientos empresariales.
- Introducción de errores intencionados.
- Errores por nerviosismo del sujeto.
- Errores causados por cierta distracción del usuario.
- Errores debidos a la negligencia del usuario.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo el error cometido por un usuario son las siguientes:

A) Errores que produzcan graves daños.

- Paralización parcial de algún proceso de negocio.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**2**	**1**	**1**

Tabla 6.43.- Valoración de Errores que produzcan daños graves.

B) Errores que produzcan daños leves.

- Posible paralización de la actividad en algún terminal.
- Pérdida de tiempo productivo en el puesto de trabajo.
- Posibilidad de volver a realizar el proceso con errores.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Alta, 3.

Gravedad de la ocurrencia: Baja, 1.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**3**	**1**	**0.3**

Tabla 6.44.- Valoración de Errores que produzcan daños leves.

C) Errores sin efectos adversos.

- No se paraliza el proceso de negocio en un ningún terminal.
- Son errores que no deberían existir pero no afectan a la actividad empresarial.
- Posibilidad de repetición del proceso donde hubiera errores.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Alta, 3.

Gravedad de la ocurrencia: Baja, 0.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**3**	**0**	**0**

Tabla 6.45.- Valoración de Errores sin efectos.

RIESGO DE ERROR DE EXPLOTACIÓN DE SISTEMAS.

DEFINICIÓN.

Este tipo de riesgo contempla todos los posibles fallos que se puedan cometer en cuanto a la instalación de nuevas aplicaciones, instalación de redes en la compañía, configuración de diversos componentes de los sistemas de información de la empresa, etc. Errores que si no son corregidos en un corto periodo de tiempo pueden ser muy peligrosos para la continuidad de los procesos de negocio de la entidad.

CAUSAS.

Las causas que pueden producir un error de explotación de los sistemas de información

empresariales son las siguientes:

- Desconocimiento de la tecnología por parte de los técnicos de explotación de sistemas.
- Errores de explotación que puedan ser inducidos.
- Falta de profesionalidad de los técnicos.
- Análisis de necesidades de la compañía en este ámbito mal realizado.

CONSECUENCIAS.

Las consecuencias que pueden surgir cuando se produce un error de explotación de los sistemas de información son las siguientes:

A) Errores de explotación con consecuencias graves en los resultados.

- Se paraliza el proceso de negocio al que afecte el error de explotación.
- Los resultados obtenidos no son los que se esperaban.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Baja, 3.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**2**	**3**	**3**

Tabla 6.46.- Valoración de Errores de explotación graves.

B) Errores de explotación con consecuencias leves en los resultados.

- Posible paralización del proceso de negocio que es afectado por el error de explotación.

- Los resultados obtenidos se parecen a los que se esperaban aunque no son correctos y hay que rectificarlos.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Alta, 3.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**3**	**2**	**0.6**

Tabla 6.47.- Valoración de Errores de explotación leves.

C) Errores de explotación que no afectan a los resultados.

- El proceso de negocio puede continuar sin problemas.
- No se contemplan daños que puedan afectar a los ingresos o imagen de la compañía.
- Los resultados que se obtienen son prácticamente iguales a los que se querían obtener, no siendo necesaria su rectificación con cierta rapidez.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Alta, 3.

Gravedad de la ocurrencia: Baja, 1.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**3**	**1**	**0.3**

Tabla 6.48.- Valoración de Errores de explotación graves.

RIESGO DE AUSENCIA DE PERSONAS CLAVE.

DEFINICIÓN.

Situación mediante la cual se produce la ausencia de ciertos empleados de la compañía, cuya función en la misma es muy importante para el desarrollo normal de los procesos de negocio empresariales. Se pueden producir situaciones muy comprometidas en el caso de que el número de ausentes sea una cifra de tamaño considerable.

Se consideran personas clave a las personas que se encargan de velar por el correcto funcionamiento de los sistemas de información de la empresa, como puede ser el mantenimiento de los servidores, el mantenimiento de la base de datos empresarial, el soporte a los distintos empleados, etc.

CAUSAS.

Las causas que pueden producir la ausencia de personas clave son las siguientes:

- Ausencia por distintos motivos personales.
- Ausencia por enfermedades.
- Ausencia por vacaciones.
- Ausencia con falsos motivos.
- Ausencia por motivos de viajes de empresa.
- Ausencias colectivas debidas a una huelga.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo la ausencia de personas en general en la compañía son las siguientes:

A) Ausencia de un número considerable de personas (de 30 a 60).

- Posible paralización de algunos procesos de negocio.
- Posible incapacidad de realizar todo el trabajo demandado.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 4.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**4**	**12**

Tabla 6.49.- Valoración de Ausencia de un número considerable de personas.

B) Ausencia media de personas en el día a día (de 10 a 10).

- Posible paralización de algunos procesos empresariales.
- Posible incapacidad de realizar todo el trabajo demandado.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**2**	**4**

Tabla 6.50.- Valoración de Ausencia de un número medio de personas.

C) Ausencia media de personas en el día a día (de 1 a 10).

- La empresa continúa su actividad normal.

- Sobrecarga de trabajo de algunos empleados.
- Posible retraso en entregas.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Alta, 3.

Gravedad de la ocurrencia: Baja, 1.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**3**	**1**	**0.3**

Tabla 6.51.- Valoración de Ausencia de un número mínimo de personas.

RIESGO DE PÉRDIDA DE MATERIAL INFORMÁTICO.

DEFINICIÓN.

Situación mediante la cual se produce el hurto o robo de cierto material informático, posiblemente durante días en los que no exista actividad empresarial en la oficina, que es vital para la continuidad de los procesos de negocio de la entidad, este material puede ir desde los servidores centrales pasando por los terminales operativos y llegando hasta las impresoras de usuario.

CAUSAS

Las causas que pueden producir el robo de material informático son las siguientes:

- Bandas organizadas que dediquen su tiempo a esta función.
- Pérdida de material inducido por ciertas personas, empleados o no.
- Descontrol a la hora de trasladar equipos o similar.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo el robo de material informático son las siguientes:

A) Robo de servidores y equipos informáticos.

- Paralización considerable de la actividad empresarial.
- Pérdida de información empresarial.
- Lesiones del personal si es robo con violencia.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 6.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**6**	**18**

Tabla 6.52.- Valoración de Robo de servidores y equipos.

B) Robo de una cantidad considerable de equipos informáticos e impresoras.

- Posible paralización de algún proceso de negocio que se haya visto muy afectado por el hurto o robo.
- Posibles lesiones del personal si es robo con violencia.
- Posible pérdida de información almacenada en los terminales sustraídos.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media/Baja, 4.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**4**	**8**

Tabla 6.53.- Valoración de Robo de una cantidad considerable de equipos.

C) Robo de algún equipo informático o impresoras.

- Paralización de la actividad llevada a cabo en los ordenadores sustraídos.
- Posible pérdida de información no guardada en dichos ordenadores.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**2**	**2**	**1**

Tabla 6.54.- Valoración de Robo de algún equipo.

RIESGO DE ROBO DE INFORMACIÓN EMPRESARIAL.

DEFINICIÓN.

Situación mediante la cual se produce el hurto, robo o extravío de cierta información empresarial, ya sea en soporte electrónico o físico, posiblemente durante días en los que no exista actividad empresarial en la oficina, que puede ser o no vital para la continuidad de ciertos procesos de negocio de la entidad, esta información puede estar almacenada desde papel, pasando por disquetes o DVD's, hasta unidades externas de gran almacenamiento.

CAUSAS.

Las causas por las cuales se puede producir el robo de cierta información empresarial son las siguientes:

- Robo llevado a cabo simplemente para causar daños a la compañía.
- Robo de cierta información para ser utilizada más tarde por la competencia.
- Pérdida negligente de información por parte de los usuarios.
- Robo de datos personales para ser utilizados más tarde con otros fines.
- Robo de información para paralizar algún proyecto de la entidad.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo el robo, hurto o extravío de cierta información empresarial son las siguientes:

A) Robo o hurto de las copias de respaldo.

- Gran dificultad de recuperación de datos empresariales.
- Posible parada de ciertos procesos de negocio.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 5.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**5**	**15**

Tabla 6.55.- Valoración de Robo de copias de respaldo.

B) Robo de información vital para la empresa.

- Posible parada de ciertos proyectos llevados a cabo por la empresa.
- Posible parada de ciertos procesos de negocio.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 3.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**3**	**6**

Tabla 6.56.- Valoración de Robo de información vital.

C) Robo de información poco relevante para la continuidad de la actividad empresarial.

- La empresa sigue funcionando sin problemas.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Media, 2.

Gravedad de la ocurrencia: Baja, 0.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**2**	**0**	**0**

Tabla 6.57.- Valoración de Robo de información poco relevante.

6.4.4.2.-RIESGOS PRODUCIDOS POR FALLOS EN LOS EQUIPOS.

RIESGO DE FALLO DE HARDWARE.

DEFINICIÓN.

Situación en la que ciertos componentes físicos de los terminales o los servidores dejan de funcionar por un tiempo indeterminado, estos componentes pueden ser por ejemplo, los discos duros, los procesadores, las placas bases, etc. Componentes sin los cuales no puede funcionar la actividad diaria de la entidad.

CAUSAS.

Las causas que pueden producir un fallo en los componentes hardware son las siguientes:

- Deformación física del disco duro.
- Cabezas de escritura tocan la superficie de los discos.
- Calentamiento de los discos duros.
- Fluctuaciones del suministro eléctrico.
- Desastres naturales.
- Sabotaje o vandalismo.
- Componentes defectuosos.
- Equipos obsoletos.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo un fallo del hardware son las siguientes:

A) Fallo grave en los servidores.

- Paralización de la actividad empresarial.
- Posible pérdida de distintos datos empresariales.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media / Baja, 4.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**4**	**12**

Tabla 6.58.- Valoración de fallo grave en los servidores.

B) Fallos en diversos terminales.

- Paralización de ciertas actividades empresariales.
- Posible pérdida de distintos datos empresariales.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 3.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**3**	**9**

Tabla 6.59.- Valoración de fallo en diversos terminales.

C) Fallo leve en algún terminal.

- Paralización del trabajo en el terminal del fallo.
- Pérdida leve de los últimos datos no guardados en el terminal.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Alta, 3.

Gravedad de la ocurrencia: Baja, 1.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**3**	**1**	**0.3**

Tabla 6.60.- Valoración de fallo leve en algún terminal.

RIESGO DE ATAQUE DE VIRUS.

DEFINICIÓN.

Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Aunque popularmente se incluye al "malware" dentro de los virus, en el sentido estricto de esta ciencia los virus son programas que se replican y ejecutan por sí mismos. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más benignos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

CAUSAS.

Las causas que pueden producir un ataque de un virus son las siguientes:

- Ataques de virus inducidos por ciertas personas.
- Ataques para causar diversos daños en la entidad.

CONSECUENCIAS.

Las consecuencias que pueden traer consigo el ataque de un virus a la compañía son las siguientes:

A) Ataque de virus causando serios daños a los sistemas de información empresariales.

- Destrucción de cierta información empresarial.
- Daños en las redes informáticas de la empresa.
- Paralización de los procesos de negocio que se vean afectados.
- Posibles daños en los servidores de la compañía.
- Imposibilidad de realizar copias de seguridad.

Incidencia económica sobre la continuidad: Total, 3.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Media, 5.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
T	**3**	**1**	**5**	**15**

Tabla 6.61.- Valoración de Ataque de virus grave.

B) Ataque de virus causando daños localizados en ciertos terminales.

- Pérdida de cierta información en los terminales afectados.
- Posibles daños en redes a nivel departamental.
- Paralización de la actividad en los terminales afectados por el virus.

Incidencia económica sobre la continuidad: Parcial, 2.

Probabilidad de ocurrencia: Baja, 1.

Gravedad de la ocurrencia: Baja, 2.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
P	**2**	**1**	**2**	**4**

Tabla 6.62.- Valoración de Ataque de virus con daños localizados.

C) Ataque de virus benignos sin demasiada importancia.

- Retraso significativo del trabajo llevado a cabo en la empresa.
- No se paraliza la actividad en ningún departamento.
- Incomodidad para realizar las tareas.

Incidencia económica sobre la continuidad: Menor, 1.

Probabilidad de ocurrencia: Alta, 3.

Gravedad de la ocurrencia: Baja, 1.

TIPO	VALOR	PROBABILIDAD	CONTINGENCIA	PESO TOTAL
M	**1**	**3**	**1**	**0.3**

Tabla 6.63.- Valoración de Ataque de virus leve.

6.5.- MEDIDAS PREVENTIVAS Y CORRECTORAS.

En este apartado se van a detallar todas las medidas preventivas que se deben tener implantadas en la compañía para cada tipo de posible riesgo, que pueda materializarse, con el fin de la reducción o desaparición del mismo. Es un tipo de medida que se toma siempre antes de que aparezca la ocurrencia del riesgo.

Como plan de acción se van a determinar todas las acciones y medidas correctoras que se deben de llevar a cabo en caso de materializarse un riesgo de los descritos anteriormente. Estas medidas se toman siempre durante o después de que haya ocurrido la contingencia.

6.5.1.- MEDIDAS PARA RIESGOS NATURALES.

MEDIDAS PREVENTIVAS PARA AFRONTAR UN INCENDIO:

Las medidas preventivas que se han tomado para afrontar un incendio son las siguientes:

- Distribución de diversos extintores a lo largo de toda la empresa.
- Distribución de diversas bocas de incendio situadas en lugares clave de la compañía.
- Instalación de sistemas automáticos de detección de humo o incendios.
- Revisiones con cierta frecuencia de la instalación eléctrica de la entidad para prevenir posibles cortocircuitos.
- Instrucciones de cómo actuar al personal en caso de producirse un incendio.
- Instalación de salidas de emergencia en lugares adecuados de la empresa.
- Señalización de caminos para la evacuación del edificio.
- Prohibición de fumar en todas las áreas de la compañía.
- Escaleras de emergencia en caso de no poder utilizar los ascensores.
- Realización de simulacros de evacuación del edificio ante una emergencia.

MEDIDAS CORRECTORAS APLICABLES ANTE UN INCENDIO:

Las medidas correctoras que se deben adoptar ante un incendio son las siguientes:

- Realizar diversas llamadas a los servicios de bomberos.
- Si el fuego es pequeño, intentar apagarlo con extintores o bocas de incendio siempre que no se ponga en riesgo la vida de nadie.
- Iniciar la evacuación del edificio por las escaleras de emergencia y nunca por los ascensores.
- Intentar que la evacuación se lleve a cabo como en los simulacros realizados de entrenamiento.
- Evaluación de daños a los sistemas de información de la compañía.
- Activar los servidores de respaldo, si es posible, para seguir dando servicio a los clientes.
- Si el fuego ha causado daños a los sistemas de información, iniciar el procedimiento de recuperación de datos y restablecimiento del sistema.
- Procedimiento de reposición de equipos y servidores dañados por el incendio.

MEDIDAS PREVENTIVAS PARA AFRONTAR UNA TORMENTA:

Las medidas preventivas que se han tomado para afrontar una tormenta son las siguientes:

- Instalación de pararrayos en la cima del edificio.
- Protecciones ante descargas eléctricas en las líneas telefónicas y de electricidad.
- Revisiones periódicas de las protecciones de las líneas telefónicas y eléctricas.
- Instrucciones al personal en cómo actuar ante situaciones de emergencia.
- Señalización de caminos para la evacuación del edificio.
- Escaleras de emergencia en caso de no poder utilizar los ascensores.

MEDIDAS CORRECTORAS APLICABLES ANTE UNA TORMENTA:

Las medidas correctoras que se deben adoptar ante una tormenta son las siguientes:

- Realizar diversas llamadas a los servicios de bomberos.
- Iniciar la evacuación del edificio por las escaleras de emergencia y nunca por los ascensores en caso de que sea necesario.
- Aplicar medidas correctoras para un incendio, no contempladas en este apartado, en caso de que éste llegase a producirse.
- Evaluación de daños a los sistemas de información de la compañía .
- Activar los servidores de respaldo, si es posible, para seguir dando servicio a los clientes.
- Iniciar procedimiento de recuperación de datos y restablecimiento del sistema si fuera necesario.
- Procedimiento de reposición de equipos y servidores si han sido dañados por la tormenta.

MEDIDAS PREVENTIVAS PARA AFRONTAR UNA INUNDACIÓN:

Las medidas preventivas que se han tomado para afrontar una anegación son las siguientes:

- Revisiones periódicas del estado del tejado del edificio.
- Revisiones periódicas del estado de todas las ventanas del edificio.
- Detectores de humedad extrema en diversos lugares de la entidad.
- Revisiones periódicas del circuito de tuberías instalado.
- Señalización de caminos para la evacuación del edificio para situaciones extremas.
- Escaleras de emergencia en caso de no poder utilizar los ascensores.
- Posesión de alguna bomba de achique en caso de necesitarla.
- Realización de simulacros de evacuación del edificio ante una emergencia.

MEDIDAS CORRECTORAS APLICABLES ANTE UNA INUNDACIÓN:

Las medidas correctoras que se deben adoptar ante una anegación son las siguientes:

- Realizar diversas llamadas a los servicios de bomberos.
- Iniciar la evacuación del edificio por las escaleras de emergencia y nunca por los ascensores en caso de que sea necesario.
- Intentar que la evacuación se lleve a cabo como en los simulacros realizados de entrenamiento.
- Evaluación de daños a los sistemas de información de la compañía.
- Activar los servidores de respaldo, si es posible, para seguir dando servicio a los clientes.
- Iniciar procedimiento de recuperación de datos y restablecimiento del sistema si fuera necesario.
- Procedimiento de reposición de equipos y servidores que hayan podido ser dañados por la anegación.

MEDIDAS PREVENTIVAS PARA AFRONTAR UN TERREMOTO:

Las medidas preventivas que se han tomado para afrontar un terremoto son las siguientes:

- Revisar periódicamente las partes del edificio más propensas a desprenderse.
- Realización de simulacros de evacuación del edificio ante una emergencia.
- Señalización de caminos para la evacuación del edificio.
- Instrucciones de cómo actuar al personal en caso de producirse un seísmo.

MEDIDAS CORRECTORAS APLICABLES ANTE UN TERREMOTO:

Las medidas correctoras que se deben adoptar ante un terremoto son las siguientes:

- Realizar diversas llamadas a los servicios de bomberos.

- Iniciar la evacuación del edificio por las escaleras de emergencia y nunca por los ascensores en caso de que sea necesario.
- Intentar que la evacuación se lleve a cabo como en los simulacros realizados de entrenamiento.
- Evaluación de daños a los sistemas de información de la compañía.
- Activar los servidores de respaldo, si es posible, para seguir dando servicio a los clientes.
- Iniciar procedimiento de recuperación de datos y restablecimiento del sistema si fuera necesario.
- Procedimiento de reposición de equipos y servidores que hayan podido ser dañados por el seísmo.

6.5.2.- MEDIDAS PREVENTIVAS PARA RIESGOS DE FALLOS EN LOS SUMINISTROS.

MEDIDAS PREVENTIVAS PARA EVITAR UN CORTE DE ELECTRICIDAD:

Las medidas preventivas que se han tomado para evitar un corte de electricidad son las siguientes:

- Apoyo de conexión en una segunda compañía eléctrica.
- Suministro eléctrico establecido por diferentes zonas para evitar apagones en todo el edificio.
- Revisiones periódicas del circuito interno de electricidad.
- Señalización mediante luces de emergencia situadas en las habitaciones, pasillos y escaleras de emergencia.
- Control entre la potencia suministrada y la necesitada por la entidad.
- Poseer un contrato de mantenimiento del suministro eléctrico.
- Tener más de un punto de entrada principal de la electricidad.
- Estar conectado a más de una subestación eléctrica.
- Estar en posesión de un mapa con todos los cables y conexiones eléctricas.

- Riguroso pago mensual de la cuota de electricidad.

MEDIDAS CORRECTORAS APLICABLES ANTE UN CORTE DE ELECTRICIDAD:

Las medidas correctoras que se deben adoptar ante un corte de electricidad son las siguientes:

- Intentar solucionar el problema desde el interior de la empresa.
- Ponerse en contacto con la compañía suministradora.
- Evaluación de daños a los sistemas de información de la compañía.
- Activar los servidores de respaldo durante el periodo que dure el corte de electricidad para dar servicio a los clientes.
- Iniciar procedimiento de recuperación de datos y restablecimiento del sistema si fuera necesario.

MEDIDAS PREVENTIVAS PARA EVITAR UN CORTE DE AGUA:

Las medidas preventivas que se han tomado para evitar un corte de agua son las siguientes:

- Instalación de varios depósitos con grandes reservas de agua.
- Revisiones periódicas de las tuberías del edificio.
- Poseer un contrato de mantenimiento de suministro de agua.
- Control de la humedad mediante sensores instalados en el edificio.
- Riguroso pago mensual de la cuota de agua.

MEDIDAS CORRECTORAS APLICABLES ANTE UN CORTE DE AGUA:

Las medidas correctoras que se deben adoptar ante un corte de agua son las siguientes:

- Intentar solucionar el problema desde el interior de la empresa.
- Ponerse en contacto con la compañía suministradora.

- Evaluación de daños a los sistemas de información de la compañía.
- Activar los servidores de respaldo durante el periodo que dure el corte de agua , en caso de que los servidores primarios dejen de prestar su servicio por recalentamiento.
- Iniciar procedimiento de recuperación de datos y restablecimiento del sistema si fuera necesario.

MEDIDAS PREVENTIVAS PARA EVITAR UN CORTE DE LAS TELECOMUNICACIONES:

Las medidas preventivas que se han tomado para evitar un corte de las telecomunicaciones son las siguientes:

- Apoyo del suministro de las telecomunicaciones en una segunda compañía.
- Rutas alternativas en caso de cortes de las líneas para la transmisión de datos.
- Desvíos automáticos de las líneas por otras rutas en caso de producirse cortes.
- Poseer un contrato de mantenimiento con la compañía de telecomunicaciones.
- Riguroso pago mensual de la cuota telefónica.

MEDIDAS CORRECTORAS APLICABLES ANTE UN CORTE DE LAS TELECOMUNICACIONES:

Las medidas correctoras que se deben adoptar ante un corte de las telecomunicaciones son las siguientes:

- Intentar solucionar el problema desde el interior de la empresa.
- Ponerse en contacto con la compañía suministradora.
- Evaluación de daños a los sistemas de información de la compañía.
- Activar los servidores de respaldo durante el periodo que dure el corte de electricidad para dar servicio a los clientes.

- Iniciar procedimiento de recuperación de datos y restablecimiento del sistema si fuera necesario.

6.5.3.- MEDIDAS PREVENTIVAS PARA RIESGOS INDUCIDOS.

MEDIDAS PREVENTIVAS PARA EVITAR UN SABOTAJE:

Las medidas preventivas que se han tomado para evitar un sabotaje son las siguientes:

- Restringir accesos a la zona de servidores de la compañía.
- Restringir accesos a zonas con información confidencial.
- Protecciones de seguridad física a las zonas mencionadas con anterioridad.
- Impedir la libre circulación de personas no identificadas por todo el edificio.
- Detallar claramente las funciones del responsable de seguridad.
- Conocer previamente las necesidades de cada empleado de la entidad.
- Controlar periódicamente la satisfacción de cada empleado dentro de la empresa.
- Actuar en consecuencia con los requisitos que el personal pueda exigir.
- Cumplimiento exhaustivo de la ley hacia el trabajador.
- Mantener a los trabajadores en unas condiciones laborables aceptables.

MEDIDAS CORRECTORAS APLICABLES ANTE UN SABOTAJE:

Las medidas correctoras que se deben adoptar ante un sabotaje son las siguientes:

- Iniciar la evacuación del edificio de los empleados que no estén participando en el sabotaje.
- Avisar a las autoridades competentes.
- Evaluación de los daños sufridos por los sistemas de información de la empresa.

- Activar los servidores de respaldo, si es posible, para seguir dando servicio a los clientes.
- Iniciar procedimiento de recuperación de datos y restablecimiento del sistema si fuera necesario.
- Procedimiento de reposición de equipos y servidores que hayan podido ser dañados debido al sabotaje.
- Cese de los empleados que hayan participado en el sabotaje.
- Presentación en los juzgados de diversas denuncias.

MEDIDAS PREVENTIVAS PARA EVITAR UN ATENTADO TERRORISTA:

Las medidas preventivas que se han tomado para evitar un atentado terrorista son las siguientes:

- Establecimiento de vigilantes de seguridad en los accesos a la compañía.
- Control de personas en todos los accesos a la entidad.
- Restringir accesos a la zona de servidores de la compañía.
- Restringir accesos a zonas con información confidencial.
- Protecciones de seguridad física a las zonas mencionadas con anterioridad.

MEDIDAS CORRECTORAS APLICABLES ANTE UN ATENTADO TERRORISTA:

Las medidas correctoras que se deben adoptar ante un atentado terrorista son las siguientes:

- Iniciar la evacuación del edificio.
- Seguir las directrices de las autoridades competentes.
- Supervisión de la zona por parte de los cedas.
- Evaluación de los daños sufridos por los sistemas de información de la empresa.
- Activar los servidores de respaldo, si es posible, para seguir dando servicio a los clientes.

- Iniciar procedimiento de recuperación de datos y restablecimiento del sistema si fuera necesario.
- Procedimiento de reposición de equipos y servidores que hayan podido ser dañados por el atentado.

MEDIDAS PREVENTIVAS PARA EVITAR UNA AMENAZA DE BOMBA:

Las medidas preventivas que se han tomado para evitar una amenaza de bomba son las siguientes:

- Establecimiento de vigilantes de seguridad en los accesos a la compañía.
- Caminos señalizados de evacuación del edificio.
- Instrucciones al personal en cómo actuar ante situaciones de emergencia.
- Instalación de salidas de emergencia en lugares adecuados de la empresa.
- Realización de simulacros de evacuación del edificio ante una emergencia.
- Escaleras de emergencia en caso de no poder utilizar los ascensores.

MEDIDAS CORRECTORAS APLICABLES ANTE UNA AMENAZA DE BOMBA:

Las medidas correctoras que se deben adoptar ante una amenaza de bomba son las siguientes:

- Iniciar la evacuación del edificio.
- Seguir las directrices de las autoridades competentes.
- Supervisión de la zona por parte de los cedas.
- En caso de explotar la bomba, aplicar medidas correctoras ante un atentado terrorista.
- Una vez se haya comprobado que no hay riesgo, volver a la actividad empresarial.

MEDIDAS PREVENTIVAS PARA EVITAR UN CASO DE VANDALISMO:

Las medidas preventivas que se han tomado para evitar una situación de vandalismo son las siguientes:

- Establecimiento de vigilantes de seguridad en los accesos a la compañía.
- Control de personas en todos los accesos a la entidad.
- Restringir accesos a la zona de servidores de la compañía.
- Restringir accesos a zonas con información confidencial.
- Protecciones de seguridad física a las zonas mencionadas con anterioridad.

MEDIDAS CORRECTORAS APLICABLES ANTE UN CASO DE VANDALISMO:

Las medidas correctoras que se deben adoptar ante una situación de vandalismo son las siguientes:

- Iniciar la evacuación del edificio.
- Avisar a las autoridades competentes.
- Evaluación de los daños sufridos por los sistemas de información de la empresa.
- Activar los servidores de respaldo, si es posible, para seguir dando servicio a los clientes.
- Iniciar procedimiento de recuperación de datos y restablecimiento del sistema si fuera necesario.
- Procedimiento de reposición de equipos y servidores que hayan podido ser dañados debido al vandalismo.
- Presentación en los juzgados de diversas denuncias.

MEDIDAS PREVENTIVAS PARA EVITAR UNA HUELGA:

Las medidas preventivas que se han tomado para evitar una huelga son las siguientes:

- Conocer previamente las necesidades de cada empleado de la entidad.
- Controlar periódicamente la satisfacción de cada empleado dentro de la empresa.
- Actuar en consecuencia con los requisitos que el personal pueda exigir.
- Cumplimiento exhaustivo de la ley hacia el trabajador.
- Mantener a los trabajadores en unas condiciones laborables aceptables.
- Conocimientos previos de posibles huelgas generales o sectoriales.
- Negociaciones y reuniones periódicas con el comité de empresa.

MEDIDAS CORRECTORAS APLICABLES ANTE UNA HUELGA:

Las medidas correctoras que se deben adoptar ante una huelga son las siguientes:

- Asumir los servicios mínimos de los trabajadores.
- Intentar dar el máximo servicio a los clientes con el personal de servicios mínimos.

6.5.4.- MEDIDAS PREVENTIVAS PARA RIESGOS INFORMÁTICOS

MEDIDAS PREVENTIVAS PARA EVITAR UN ERROR DE DESARROLLO:

Las medidas preventivas que se han tomado para evitar un error de desarrollo son las siguientes:

- Repartir las tareas de programación en diferentes módulos, para así poder trabajar en equipo y sea más fácil la reparación de posibles errores.
- Realización de diferentes pruebas para comprobar que la aplicación desarrollada funciona correctamente.
- Garantizar que el equipo de prueba de la aplicación está formado por individuos distintos a los programadores de la misma.

- Controlar el estricto cumplimiento de las normas de seguridad de acceso a la información para impedir en la programación la posibilidad de acceso a los datos sensibles o confidenciales.
- Realizar controles de seguridad en la fase de pruebas.
- Obtener garantías de éxito de la aplicación a una tercera compañía en caso de que el desarrollo sea subcontratado.
- Controlar siempre los privilegios de acceso a la aplicación y la integridad de los datos que gestiona la misma.
- Utilizar siempre sistemas operativos que tengan una buena imagen en el mercado actual.
- Implantación de un historial con los movimientos de desarrollo que lleva a cabo cada programador, para en caso de fallo conocer quien lo ha cometido.
- Impedir el paso directo de modificaciones de aplicaciones al entorno de producción, sin contrastarlas previamente en un entorno de test.
- Realización de la aplicación en tres entornos distintos (Producción, test e instalación).
- Dividir responsabilidades entre los controladores del correcto funcionamiento de la aplicación.
- Realizar un control de calidad de la aplicación una vez que haya pasado las pruebas con éxito.

MEDIDAS CORRECTORAS APLICABLES ANTE UN ERROR DE DESARROLLO:

Las medidas correctoras que se deben adoptar ante error de desarrollo son las siguientes:

- Identificar rápidamente al programador que ha cometido dicho error.
- Evaluación por parte del responsable de la aplicación de las causas por las.
- cuales el programador ha cometido el error.
- Intentar reparar dicho error en el menor tiempo posible.
- Realizar las pruebas necesarias para garantizar que el error ha desaparecido
- por completo.

- Instalar la aplicación saneada en los terminales que la requieran

MEDIDAS PREVENTIVAS PARA EVITAR UN ERROR DE MANTENIMIENTO:

Las medidas preventivas que se han tomado para evitar un error de mantenimiento son las siguientes:

- Contratación de técnicos altamente cualificados.
- Exigencia de garantías en cuanto a tiempo de entrega a los suministradores de material informático.
- Pruebas por parte de los usuarios para comprobar que su necesidad ha sido satisfecha por el técnico.

MEDIDAS CORRECTORAS APLICABLES ANTE UN ERROR DE MANTENIMIENTO:

Las medidas correctoras que se deben adoptar ante error de mantenimiento son las siguientes:

- Identificar rápidamente a la persona de mantenimiento que ha cometido dicho error.
- Evaluación por parte del responsable de mantenimiento de las causas por las cuales el empleado ha cometido el error.
- Intentar reparar dicho error a través de la persona que lo cometió o mediante otra en el menor tiempo posible.
- Realizar las pruebas necesarias para garantizar que el error ha desaparecido por completo.
- Comprobación por parte del usuario.

MEDIDAS PREVENTIVAS PARA EVITAR UN ERROR DE EXPLOTACIÓN:

Las medidas preventivas que se han tomado para evitar un error de explotación son las siguientes:

- Contratación de técnicos altamente cualificados.
- Pruebas por parte de los usuarios para comprobar que su necesidad ha sido satisfecha por el técnico.
- Utilizar siempre sistemas operativos que tengan una buena imagen en el mercado actual.
- Impedir el paso directo de modificaciones en la explotación de sistemas al entorno de producción, sin contrastarlas previamente en un entorno de test.
- Realización de la explotación en tres entornos distintos (Producción, test e instalación).
- Obtener garantías de éxito de la aplicación a una tercera compañía en caso de que la explotación de sistemas sea subcontratada.
- Controlar siempre los privilegios de acceso a los sistemas y a la integridad de los datos que gestiona los mismos.
- Realización de diferentes pruebas para comprobar que el sistema funciona correctamente.
- Garantizar que el equipo de prueba del sistema está formado por individuos distintos a los explotadores del mismo.

MEDIDAS CORRECTORAS APLICABLES ANTE UN ERROR DE EXPLOTACIÓN:

Las medidas correctoras que se deben adoptar ante error de explotación son las siguientes:

- Identificar rápidamente a la persona de explotación que ha cometido dicho error.
- Evaluación por parte del responsable de explotación de las causas por las cuales el empleado ha cometido el error.

- Intentar reparar dicho error a través de la persona que lo cometió o mediante otra en el menor tiempo posible.
- Realizar las pruebas necesarias para garantizar que el error ha desaparecido por completo.
- Comprobación por parte del usuario.

MEDIDAS PREVENTIVAS PARA EVITAR UN ERROR DE USUARIO:

Las medidas preventivas que se han tomado para evitar un error de explotación son las siguientes:

- Formar de una manera adecuada al usuario en el uso de las aplicaciones que va a utilizar.
- Poseer manuales explicativos, sencillos y precisos acerca de las aplicaciones empresariales.
- Capacitar al usuario de las aplicaciones ante posibles cambios que puedan surgir en los procesos de negocio de la entidad.
- Controlar los posibles errores repetitivos que puedan cometer los usuarios.
- Asegurarse que las aplicaciones que utilizan los usuarios han pasado todas las pruebas de validación.
- Prestar ayuda a las personas que aún no son expertas en ciertas aplicaciones.

MEDIDAS CORRECTORAS APLICABLES ANTE UN ERROR DE USUARIO:

Las medidas correctoras que se deben adoptar ante error de usuario son las siguientes:

- Esperar a que el usuario se comunique con el responsable de seguridad o mantenimiento de sistemas y exprese su acción incorrecta.
- Atender lo más rápido posible al usuario que ha cometido el error.
- Evaluación por parte del responsable de las causas por las cuales el empleado ha podido cometer el error.
- Intentar reparar dicho error a la mayor brevedad posible.

- Realizar las pruebas necesarias para garantizar que el error ha desaparecido por completo.
- Asegurarse que el usuario ha tomado nota de su error para que no vuelva a cometerlo.

MEDIDAS PREVENTIVAS PARA EVITAR UN ROBO O PÉRDIDA DE EQUIPOS:

Las medidas preventivas que se han tomado para evitar un robo o una pérdida de equipos son las siguientes:

- Tener asegurados por lotes todos los equipos informáticos de la entidad.
- Tener instalados en ciertos lugares, anclajes en los equipos informáticos.
- Impedir la libre circulación de personas por dentro de la compañía.
- Tener controles de acceso a la entidad las 24 horas del día.
- Tener instaladas altas medidas de protección física en la sala de servidores.
- Restringir el acceso a ciertas personas a la sala de servidores.
- Tener actualizado el inventario de activos por cada departamento empresarial.
- Estar en posesión de equipos u otro material informático de repuesto para las posibles sustituciones.
- En caso de traslados de equipos, contratar garantías ante posibles contingencias que puedan ocurrir.
- Suprimir datos confidenciales de los equipos en caso de que se vaya a realizar un traslado de los mismos.
- Tener personal de la empresa presente en los posibles traslados que se puedan llevar a cabo.

MEDIDAS CORRECTORAS APLICABLES ANTE UN ROBO O PÉRDIDA DE EQUIPOS:

Las medidas correctoras que se deben adoptar ante el robo o la pérdida de equipos son las siguientes:

- Avisar al responsable de seguridad por parte de la primera persona que se percate de una falta de material informático.
- Preguntar al personal de la empresa sobre el extravío o robo del material.
- Anotar la pérdida en el libro de incidencias de la compañía.
- Reposición del material informático extraviado o hurtado.

MEDIDAS PREVENTIVAS PARA EVITAR UN ROBO O PÉRDIDA DE DOCUMENTACIÓN:

Las medidas preventivas que se han tomado para evitar un robo o pérdida de documentación son las siguientes:

- Información almacenada en papel que ya no contenga valor empresarial debe de ser destruida.
- Información almacenada en formato electrónico que ya no sea de uso para la empresa debe de ser destruida.
- En caso de traslados de equipos, contratar garantías ante posibles contingencias que puedan ocurrir
- Controlar todas las salidas y llegadas de información para la empresa, sobre todo ante el uso de las copias de respaldo.
- Tener personal de la empresa presente en los posibles traslados que se puedan llevar a cabo.
- Impedir la libre circulación de personas por dentro de la compañía.
- Tener controles de acceso a la entidad las 24 horas del día.
- Tener instaladas altas medidas de protección física en la sala de servidores.
- Restringir el acceso a ciertas personas a la sala de servidores.

MEDIDAS CORRECTORAS APLICABLES ANTE UN ROBO O PÉRDIDA DE DOCUMENTACIÓN:

Las medidas correctoras que se deben adoptar ante el robo o la pérdida de documentación son las siguientes:

- Avisar al responsable de seguridad por parte de la primera persona que se percate de una falta de documentación empresarial.
- Preguntar al personal de la empresa sobre el extravío o robo de la documentación.
- Anotar la pérdida en el libro de incidencias de la compañía.
- Volver a generar la información si es posible.

MEDIDAS PREVENTIVAS PARA EVITAR UNA AUSENCIA DE PERSONAS CLAVE:

Las medidas preventivas que se han tomado para evitar una ausencia de personas clave son las siguientes:

- Tener siempre a un segundo responsable en puestos de alta responsabilidad.
- Controlar los periodos de ausencias entre los diferentes puestos de la compañía.
- Evitar ausencias simultáneas del primer y segundo responsable de un determinado puesto.

MEDIDAS CORRECTORAS APLICABLES ANTE UNA AUSENCIA DE PERSONAS CLAVE:

Las medidas correctoras que se deben adoptar ante la ausencia de personas clave son las siguientes:

- Se investigan los motivos por los cuales el primer titular del puesto no se encuentra en la oficina.
- Se investigan los motivos por los cuales el segundo titular del puesto no se encuentra en la oficina.
- Se busca a una persona cualificada que pueda cubrir el puesto por un determinado tiempo hasta que retornen el primer o segundo titular a la compañía.

MEDIDAS PREVENTIVAS PARA EVITAR UN FALLO DE HARDWARE:

Las medidas preventivas que se han tomado para evitar un fallo de hardware son las siguientes:

- Controles periódicos del estado de situación de todo el hardware de la compañía.
- Poseer hardware sustitutivo en las oficinas de la empresa, para así evitar demandarlo al fabricante.
- Establecer un tiempo máximo de envío de los productos demandados con la compañía suministradora.
- Tener un contrato de mantenimiento con la compañía suministradora.
- Mantener los equipos a temperaturas adecuadas.
- Controles de la corriente eléctrica suministrada a cada equipo mediante enchufes inteligentes.

MEDIDAS CORRECTORAS APLICABLES ANTE UN FALLO DE HARDWARE:

Las medidas correctoras que se deben adoptar ante un fallo de hardware son las siguientes:

- El usuario se pone en contacto con el responsable de mantenimiento.
- Un empleado de mantenimiento hace una valoración del problema existente.
- Si es posible el problema se resuelve en el instante mediante el empleado de mantenimiento.
- Si el problema es de causa mayor, se lleva el equipo al taller de mantenimiento y se le sustituye temporalmente el equipo por otro de reemplazo.
- Una vez solucionado el problema se le devuelve su equipo al usuario.
- El usuario sigue trabajando con normalidad.

MEDIDAS PREVENTIVAS PARA EVITAR UN ATAQUE DE VIRUS:

Las medidas preventivas que se han tomado para evitar un ataque de virus son las siguientes:

- Utilizar un antivirus en cada equipo como norma general.
- Utilizar antivirus que detecte y elimine los virus que se puedan presentar.
- Utilizar antivirus que detecten virus en archivos ejecutables, procesadores de texto y hojas de cálculo.
- Actualizar con cierta frecuencia el antivirus implantado en cada equipo.
- Utilizar software de antivirus conocido en el mercado de la informática.
- Probar el software adquirido en entornos aislados.
- Prohibir con toda contundencia la utilización de software ilegal.
- Prohibir exhaustivamente los programas que no tengan un origen claro.
- Realizar chequeos semanales de todos los equipos de la empresa.
- No abrir bajo ningún concepto archivos adjuntos de un correo electrónico que parezca sospechoso.
- Realizar periódicamente copias de seguridad de los archivos del sistema.

MEDIDAS CORRECTORAS APLICABLES ANTE UN ATAQUE DE VIRUS:

Las medidas correctoras que se deben adoptar ante un ataque de virus son las siguientes:

- El usuario se pone en contacto con el responsable de seguridad y le informa que ha sufrido un ataque de virus en su terminal.
- Si no hay pérdida de archivos y el virus solo afecta al sistema, se procede a la restauración del equipo y eliminación del virus.
- Si además hay pérdida de archivos, se realiza lo mismo que en el punto anterior, y a parte se recuperan los datos que se han perdido a través de las copias de respaldo de la información.
- Una vez saneado el problema, el usuario continúa con su actividad en su terminal.

7

CENTRO DE ATENCIÓN A USUARIOS

7.- CENTRO DE ATENCIÓN A USUARIOS (CAU).

7.1.- GESTIÓN DE INCIDENCIAS.

La Gestión de Incidencias es el proceso de detectar y resolver problemas o incidencias en el centro de servicios informáticos.

Es muy importante distinguir, desde el principio, las incidencias de las peticiones; los problemas son anomalías en el funcionamiento normal o esperado, que afecten a algún componente de un sistema informático, tanto si se produce como si no una interrupción en el servicio; las peticiones consisten en solicitudes de cambio, por parte de los usuarios, tanto en el hardware como en el software, cambios que han de ser gestionados y controlados por la función informática. También se distinguen las incidencias de los cambios en que las primeras tienen siempre la consideración de urgentes y han de ser identificadas y encauzadas rápidamente por el CAU, mientras que la conveniencia de los segundos puede ser analizada con tiempo por las personas adecuadas y no son responsabilidad exclusiva del CAU.

Las funciones y actividades principales de la gestión de incidencias deben consistir en:

- Definición y mantenimiento de los procedimientos de gestión de incidencias y aseguramiento de los recursos humanos y técnicos para llevarlos a cabo.
- Facilitar el servicio informático requerido para la tramitación de operaciones en cualquier punto de la organización.
- Resolver las incidencias producidas por errores, averías o cambios operativos, tanto de hardware como de software.
- Información y control del estado del problema, así como elaboración de los informes pertinentes a dirección.
- Documentar las actividades realizadas en cada caso, estableciendo procedimientos para la resolución de incidencias conocidas y un sistema adecuado de previsión.

- Establecer un único punto de entrada para el tratamiento y solución de las incidencias, que funcione de modo autónomo y con un impacto mínimo en la organización.
- Establecer los medios oportunos (herramientas) que rentabilicen al máximo los conocimientos de los técnicos informáticos y los ponga al alcance de la organización.

La misión del CAU ha de incluir el establecimiento de los procedimientos correspondientes al sistema de gestión de incidentes y la relación de las actividades del mismo, así como la gestión global de todas las actividades en niveles inferiores, asegurando el cierre del bucle operativo con el usuario y un seguimiento del estado de resolución de problemas en todo instante.

Esta misión se lleva a cabo mediante tipos de actividades diferentes que pueden ser realizadas por una persona, varias o por distintos equipos.

Las etapas indispensables para la resolución de una incidencia o problema son las siguientes:

1ª etapa.- Detección del problema.

El primer evento que puede representar una gran pérdida de tiempo y que puede producir una crisis es donde y como se detecta una incidencia. Es absolutamente imprescindible que el problema sea reportado, con todo detalle, tan pronto como sea detectado. Cualquiera que se encuentre con un problema es responsable de la identificación del mismo y de comunicarlo al CAU con la descripción de todos los detalles y circunstancias que puedan ayudar a su solución.

Conviene tener en cuenta en esta etapa que un resultado inevitable del desarrollo y utilización de la tecnología de la información con estaciones de trabajo de mas fácil uso, incrementan la dificultad para la identificación del problema y de como solucionarlo. De ahí que se haga imprescindible que todo usuario disponga de un procedimiento de

soporte accesible y claro, además de ser periódicamente revisado. En la empresa el medio a utilizar para informar de la incidencia es la empresa.

2ª etapa.- Registro del problema.

Cuando se recibe una llamada para reportar una incidencia al CAU, el primer paso es la identificación de la gravedad de la misma y su inmediato registro, con objeto de que sea encaminada hacia la persona o función idónea para su resolución con la indicación de la prioridad de forma que contribuya a acelerar su solución. La coordinación de la incidencia por parte del CAU es la clave para el éxito del proceso de resolución de un problema, así pues, la importancia que se le dé al mismo y su posición en la organización son objetivos que deben cuidarse de manera especial

Las preguntas indispensables que debe formularse el CAU son:

- ¿Está realmente bien descrito el problema en el informe?
- ¿Cuál es la gravedad del mismo?
- ¿Quién es la persona idónea para resolver el problema?
- ¿Cuánto tiempo se estima necesario para su resolución?
- ¿Existe una clara discrepancia entre el tiempo para solucionar el problema y el tiempo límite para la terminación de los trabajos a los que afecta?

Todo esto indica que el CAU debe estar coordinado por alguien con un buen conocimiento de la tecnología de la información utilizada y de las personas responsables de las distintas funciones de soporte dentro de los sistemas de información.

3ª etapa.- Determinación y solución de la incidencia.

Lo primero que debe hacerse es identificar y aislar, en caso necesario, el componente causante del problema. En los casos en los que se sospeche inicialmente la existencia de un virus, sea cual sea el tipo, se deberán arrancar las medidas para aislar el puesto de trabajo y eliminar el virus, así como analizar su posible extensión a otros elementos de la red.

En esta etapa es importante dejar constancia de la lógica seguida, ya que muchos problemas se presentan repetidamente. Es también importante que después de unos primeros meses queden bien definidos los niveles de determinación de problemas:

- 1er. Nivel:
  Problemas en procedimientos, aplicaciones u operaciones del usuario en el terminal que, en general, son detectados por el mismo usuario. Deberían resolverse en su mayoría en cuanto se termine la descripción.

- 2do Nivel:
  Problemas relacionados con componentes del sistema tales como hardware, software básico o software de aplicaciones. La solución en este caso deberá ser proporcionada desde Sistemas.

- 3er. Nivel:
  Problemas que se presentan simultáneamente en más de un área específica o problemas intermitentes de difícil identificación. Las personas indicadas para el seguimiento y posterior solución son los Administradores de Sistemas. En este caso es muy posible que sea necesario establecer contacto con las casas suministradoras, tanto de hardware como de software.

4ª etapa.- Informe de la incidencia.

El informe final de la incidencia debe reflejar las distintas fases que se acaban de enumerar. Así mismo deben quedar registradas estas fases del procedimiento de resolución de la incidencia para que puedan realimentar y enriquecer las soluciones disponibles en el CAU.

También debe servir para medir la satisfacción de los usuarios en cuanto al servicio proporcionado a los mismos, indicar las posibles desviaciones observadas, informando de la razón de las desviaciones y establecer el estado general de los servicios y las peticiones de los nuevos servicios.

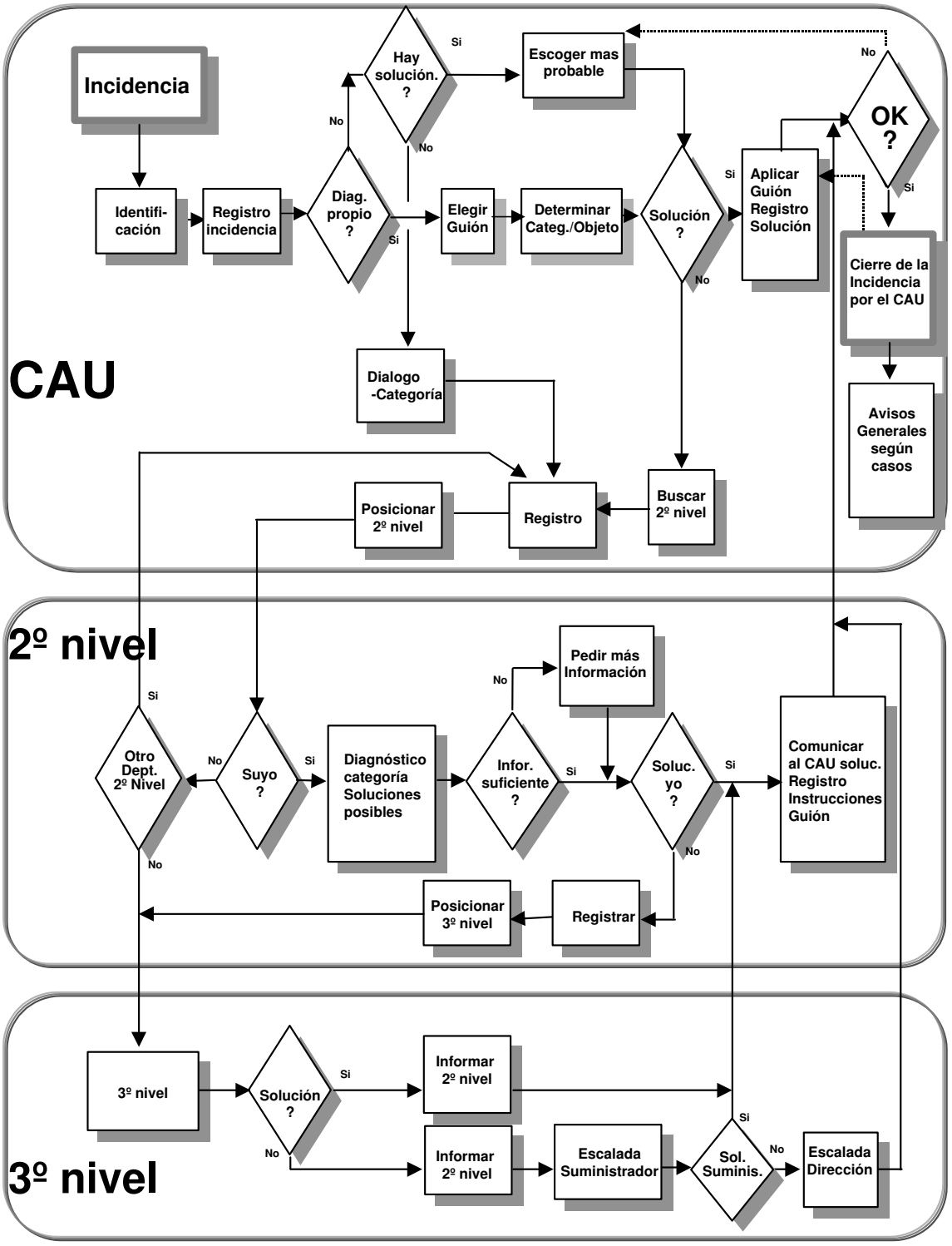

Tabla 7.1.- Esquema de funcionamiento del CAU.

7.2.- PLAN DE ACCIÓN.

1.- Evaluar situación actual.
2.- Definir el proceso de gestión de problemas.
3.- Fijar responsabilidades.
4.- Seleccionar el software de gestión.
5.- Selección de personal
6.- Integrar el inventario de informática en el CAU.
7.- Diseñar informes de gestión.
8.- Establecer Nivel de Servicio.
9.- Expandir el servicio.

7.2.1.- EVALUAR SITUACIÓN ACTUAL.

Para poder introducir cambios en el funcionamiento del CAU se debe analizar la situación actual del servicio, lo que permitirá evaluar la oportunidad del mismo y estimar el coste y recursos necesarios para su implantación. Se comenzará con la recopilación de la información disponible acerca de las características técnicas y otros aspectos de la plataforma y escenario donde se desenvuelve el trabajo de los usuarios.

- Infraestructura tecnológica.
- Herramientas utilizadas.
- Grado de dificultad de uso.
- Redes de comunicaciones.
- Grado de utilización de la infraestructura.
- Grado de movilidad de los usuarios.
- Distribución horaria de la utilización de herramientas.
- Grado de experiencia.
- Distribución geográfica.

Todo aquello que pueda afectar a la consecución del proyecto: objetivos preliminares, riesgos, etc.

7.2.2.-DEFINIR EL PROCESO DE GESTIÓN DE PROBLEMAS.

El establecimiento de un servicio como el CAU que puede atender a todos los departamentos de la organización, debe responder a unas expectativas de Calidad y Nivel de Servicio que deben estar perfectamente definidos. En líneas generales, el comportamiento básico del CAU responde a unas características similares en todas las organizaciones.

Una incidencia la inicia un usuario que tiene un problema con su equipo informático y en consecuencia se pone en contacto con el CAU. La incidencia puede afectar sólo al usuario que efectúa la llamada o a un colectivo del que forma parte.

Con la comunicación telefónica, la persona que atiende la llamada debe solicitar la información necesaria de forma estructurada para que sea posible identificar al usuario que origina la llamada así como su localización y dependencia. Después recabará todos los datos necesarios sobre los síntomas de la incidencia (efecto producido, sobre que componente, etc.). Es importante valorar la gravedad de la incidencia.

El CAU procederá a registrar la apertura de la incidencia con toda la información que solicite la propia aplicación.

- Origen de la incidencia.
- Fecha y hora en que se produce.
- Tipo de incidencia.
- Descripción.
- Estado en que se encuentra (pendiente, escalado, en curso, etc.).

Si la solución la puede suministrar el profesional del CAU, se la comunica al usuario, y cierra la incidencia, registrando el cierre. El cierre de la incidencia debe de contener:

- Fecha y hora del cierre.
- Persona que suministra la solución.
- Descripción, lo más detallada posible, de la solución aportada.

Si la solución la tiene que proporcionar una persona ajena al CAU, se registra el estado de la incidencia y se pasa al segundo nivel.

La comunicación con el segundo nivel se hará mediante vía telefónica.

El segundo nivel puede tomar una de las siguientes acciones:

- Resolver la incidencia con la información recibida.
- Ponerse en contacto con el usuario para recabar más información y resolver la incidencia.
- En caso necesario visitar al usuario para solucionar el problema in-situ.
- Cuando la situación lo requiera, escalará consultas a un tercer nivel, que en general será externo a la organización.
- En todos los casos informará al CAU del estado en que se encuentra la incidencia, de la solución adoptada y del cierre de la misma. En su caso, deberá comunicar al CAU la información complementaria sobre el problema.

Cuando la solución esté aceptada e implantada por el usuario se procederá a cerrar y registrar el cierre de la incidencia.

El CAU es el responsable de realizar el seguimiento de las incidencias, así como de mantener al usuario informado de los problemas abiertos que le correspondan.

7.2.3.-FIJAR RESPONSABILIDADES.

Las funciones de gestión, supervisión y evaluación del servicio las asume el personal de la propia empresa aunque todas, o la mayoría, de las tareas operativas estén delegadas en el personal contratado.
Las áreas de actuación se deben dirigir sobre todo a:

- La divulgación del servicio.
- Establecer un sistema de información permanente respecto a los objetivos y a la situación del servicio.
- Recoger, valorar y estructurar las posibles cambios de las funciones del servicio CAU, que respondan a las peticiones o expectativas de usuarios de forma abierta, que permita la incorporación de nuevas funciones en el futuro y que pueda aumentar la calidad del servicio prestado.

Para ello se deben llevar a cabo las siguientes actividades:

- Mantener contactos regulares con usuarios.
- Recoger, evaluar y realizar o tramitar, en su caso, las peticiones de los usuarios.
- Realizar revisiones periódicas del funcionamiento.
- Realizar el plan de nivel de servicios.
- Analizar la disponibilidad de los servicios.
- Analizar y distribuir los informes de gestión.
- Informar regularmente a la Dirección.
- Supervisar la vigencia de los procedimientos y de la normativa.

Para regular el funcionamiento del Servicio, se deben definir los procedimientos que regulen las relaciones internas y con los departamentos de la organización y con otras organizaciones, (proveedores de hardware, software y mantenimiento).

7.2.4.- SELECCIÓN DEL SOFTWARE DE GESTIÓN.

Es de desear que el CAU funcione como un organismo inteligente, con capacidad de aprender, de forma que la experiencia pueda ser acumulada con independencia de las personas que lo forman. Para ello es imprescindible la utilización de una aplicación específica de Gestión de CAU, que permita a los profesionales el registro y consulta de problemas y soluciones, capacitándolos además para suministrar otras funciones complementarias.

Para la realización de las funciones encomendadas a la gestión del CAU es recomendable la utilización de un software específico que facilite su funcionamiento. Este software debe responder a las necesidades del CAU en cuanto a su función de ayuda a los usuarios de la empresa y a la gestión de esta ayuda. Para la selección de este software se han de valorar, entre otras, las siguientes características:

- Capacidad de análisis y control de las incidencias.
- Facilidades para la formación.
- Control de calidad del Servicio.
- Capacidad de aprendizaje.
- Capacidad para integrar el inventario existente.
- La gestión de costes.
- Medida de la efectividad del personal del CAU.
- Medios que faciliten el análisis de las posibles carencias en la formación de los usuarios.
- El análisis de proveedores (calidad de equipamiento).
- Medir el comportamiento de las compañías proveedoras de mantenimiento.
- Gestión de rendimiento (calidad y tiempo de aplicación de soluciones).
- Registro de incidencias.
- Registro de soluciones.
- Medida de satisfacción de usuarios.
- Medida de utilización del servicio.
- Gestión de informes.

Se estudiarán las características del software ya instalado y se analizarán las necesidades reales de éste. Si es posible la adaptación, se llevará a cabo un plan de implantación. Si la adaptación a las necesidades reales no fuese posible, será necesario analizar las ofertas del mercado aplicando los criterios anteriores y los requerimientos que la Dirección y los técnicos a cargo del servicio sugieran.

7.2.5.- SELECCIÓN DE PERSONAL DEL CAU.

Hay un aspecto fundamental en el apartado de personal. La procedencia, selección y forma de contratación del personal que va a prestar sus servicios en el departamento: puede ser de la propia empresa, externo a ella o formar parte de una contratación de outsourcing con una empresa de servicios.

El personal encargado del CAU es de la propia empresa, teniendo así toda la información necesaria sobre esta y sus actividades de negocio, pudiendo así decidir las prioridades de las incidencias en todo momento.

7.2.6.- INTEGRAR EL INVENTARIO DE INFORMÁTICA.

Para el buen funcionamiento del CAU, se deberá incluir la adaptación del inventario con el software seleccionado, lo cual ayudará a valorar las medidas de rendimiento de suministradores y mantenimiento de los sistemas.

7.2.7.- DISEÑAR INFORMES DE GESTIÓN.

Los informes de gestión están encaminados al control de la funcionalidad del CAU y a la evaluación del servicio prestado. El software de gestión del CAU debe de facilitar de la forma más automática posible la elaboración periódica de estos informes y estar abierto a las peticiones de información esporádicas. Normalmente los informes están basados en estadísticas y series temporales. Aunque la disponibilidad de información estructurada depende fundamentalmente del software de gestión utilizado, debería estar disponible información para la generación de informes, como pueden ser:

- Distribución del número total de incidencias.
- Distribución por tipo y origen (fabricante o suministrador) de componente afectado, hardware, software básico, software de aplicaciones, periferia y conectividad y comunicaciones.
- Duración de las incidencias, máxima, mínima y media.
- Distribución del suministro de soluciones, CAU, nivel 1º nivel 2.
- Distribución de incidencias por departamento, oficina, emisora, etc.
- Eficacia de empresas de mantenimiento.
- Calidad de productos suministrados, hardware, software, periferia.

7.2.8.- ESTABLECER NIVEL DE SERVICIO

El CAU se relaciona con todos los departamentos de la empresa. Esta horizontalidad obliga a un establecimiento muy claro de las reglas del juego. No todos los departamentos son iguales, ni tienen el mismo horario de trabajo, ni tienen el mismo nivel de formación, ni su trabajo es igual de crítico para la empresa.

Se deben establecer unos Niveles de Servicio que respondan a las expectativas de un número representativo de usuarios.

El establecimiento de un Nivel de Servicio no se hace de forma unilateral ni significa que todos los departamentos deban aceptarlo. El nivel de servicio se ha de negociar con los usuarios. En el caso de los departamentos más críticos se negociaran cláusulas específicas. En la negociación deberá tenerse muy en cuenta los costes que representa el ampliar los turnos de servicio, o establecer turnos en días festivos, o bajar los tiempos empleados en la solución de problemas, etc.

8

PLANIFICACION REAL DE LAS ACTIVIDADES

8.- PLANIFICACION REAL DE LAS ACTIVIDADES.

Las tareas que se han identificado y su planificación a lo largo del proyecto son:

- Plan de gestión del proyecto: Se identificara el ámbito del proyecto, objetivos y metodología a utilizar.
- Análisis de la empresa: descripción de todos los aspectos concernientes a la empresa, desde la lógica de negocio hasta la arquitectura lógica y hardware.
- Determinación de aplicaciones y datos críticos: Descripción de aplicaciones críticas y relación con las aplicaciones y datos de la empresa.
- Seguridad Física y Lógica: Descripción y desarrollo de los diversos sistemas de seguridad para garantizar la integridad y la confidencialidad de los bienes y documentos que tiene la empresa en su haber.
- Análisis de riesgos: investigación de los riesgos a los que están expuestos los sistemas de información y recomendar las medidas apropiadas que deberán adaptarse para controlar dichos riesgos.
- Medidas Preventivas: Desarrollo de las medidas tomadas en cuenta por la empresa.
- Medidas Correctoras: Desarrollo de medidas de actuación ante la aparición de cualquier riesgo.
- Redacción de la memoria: Etapa que realizada durante todo el desarrollo del proyecto.

NOMBRE DE LA TAREA	DURACION	INICIO	FIN
Plan de gestión del proyecto	56 días	19/10/2007	04/01/2008
Análisis de la empresa	41 días	26/10/2007	21/12/2007
Determinación de aplicaciones y datos	49 días	07/11/2007	20/02/2008
Seguridad física y lógica	76 días	26/11/2007	31/01/2008
Soporte de la información	95 días	17/01/2008	28/05/2008
Análisis de riesgos	79 días	11/01/2008	30/04/2008
Medidas preventivas	39 días	01/05/2008	24/06/2008
Medidas correctoras	45 días	09/05/2008	10/07/2008
Redacción de la memoria	188 días	30/10/2007	17/07/2008

Tabla 8.1.- Planificación del proyecto.

9

CONCLUSIONES

9.- CONCLUSIONES

La realización del proyecto ha implicado un arduo trabajo en recopilación de información de numerosas empresas, donde ha habido que conocer el funcionamiento del sistema de información y la lógica de negocio para poder comprender la seguridad en un amplio conjunto.

La dificultad de sintetizar las distintas etapas y recursos que se ven implicados en este tipo de plan es muy grande. Es muy importante realizar un buen análisis de los riesgos que puede sufrir cada uno de los recursos y sistemas de la organización. Así como conocer profundamente lo que es un plan de seguridad, distinguiendo dos aspectos fundamentales, contingencias y recuperación, y como se deben implementar para la realización del proyecto.

La primera etapa del proyecto ha sido una visión general de la empresa, sistema de información y lógica de negocio para poder aplicar un plan de seguridad, esto llevó a poseer un gran volumen de información que había que sintetizar, desarrollando así la información lo más concreta y exacta posible.

Una vez que va evolucionando el proyecto, van surgiendo nuevas ideas o métodos que hay que ir modificando, aspectos de la empresa que hay que tener más en cuenta para el desarrollo del plan.

Además de la adquisición de conocimientos técnicos y de gestión de seguridad adquiridos gracias a la realización del proyecto, hay una serie de conclusiones a las que se ha llegado una vez se tiene la visión global que proporciona el haber realizado un proyecto como éste. Las conclusiones más importantes son las siguientes:

La seguridad afecta a todos los elementos de la organización: a sus procesos de negocio, los cuales deben ser seguros, a los recursos de la compañía, a los activos tangibles e intangibles de la misma. Un buen plan de seguridad elaborado a tiempo puede llegar a ahorrar mucho tiempo y dinero.

El haber podido realizar el plan de seguridad de una compañía en toda su extensión, desde las tareas de análisis hasta la implantación última, ha permitido al autor adquirir una visión completa e integral de la compañía, de los procesos que desarrolla, de los recursos con los que cuenta, las interacciones entre los mismos, cuáles son los procesos y recursos críticos y cuáles son más accesorios.

Ha sido una experiencia gratificante y el sentimiento de realización es pleno ya que todos los conocimientos adquiridos y aplicados han quedado plasmados en un plan de seguridad eficiente, fiable y eficaz.

10

BIBLIOGRAFÍA

10.- BIBLIOGRAFÍA

Las páginas web consultadas para la realización del proyecto son las siguientes:

- www.mailxmail.com/curso/informatica/backup/capitulo7.htm
- www.alertas.red.es/seguridad/ver_pag.html?tema=S&articulo=1&pagina=2
- www.hispasec.com
- http://securityfocus.com
- http://secinf.net

Libros y documentos consultados para la realización del proyecto son los siguientes:

[CAMP08] Camps, Mateo. Planteamiento general de la problemática de seguridad en los Sistemas de Información. Sin editorial. Madrid. 2008.

[CAMP08] Camps, Mateo. Gestión de la información en los entornos estratégico, táctico y operativo. Sin editorial. Madrid. 2008.

[INFO05] Sin autor. Information technology, Security techniques, Code of practice for information security management. Sin editorial. 2005.

[BARR95] Barranco de Areba, Jesús. "Metodología del Análisis Estructurado de Sistemas. UPCO. 1995.

[HERN00] Hernández Goya, Candelaria. Criptología y Seguridad de la información. Rama. 2000.

[MCCA02] Mary Pat McCarthy y otros. Seguridad Digital. McGraw-Hill.2002.

[PESO03] Peso Navarro, Emilio del. Servicios de la Sociedad de la Información: comercio electrónico y protección de datos. Díaz de Santos. 2003.

[STSI94] Steven Shaffler y Alan Simon. Network Security. AP Professional. 1994.

11

ANEXOS

11.1.- ANEXO A. VALORACIÓN REAL DEL PROYECTO.

Para esta parte se supondrá que el proyecto ha sido realizado por un Ingeniero Informático trabajando 11,86 horas semanales durante 35 semanas, haciendo un total de 415 horas de trabajo. Suponiendo que su salario sea de 30 €/hora. El coste de personal ascendería a 12,450 € para la totalidad del proyecto. El número de horas que se han empleado en la realización del presente proyecto se puede observar de forma más detallada en la siguiente tabla:

NOMBRE DE LA TAREA	HORAS
Plan de gestión del proyecto	37
Análisis de la empresa	92
Determinación de aplicaciones y datos	52
Seguridad física y lógica	85
Soporte de la información	12
Análisis de riesgos	112
Medidas preventivas	12
Medidas correctoras	13
Redacción de la memoria	---

Tabla 11.1.- Horas empleadas para desarrollar el proyecto.

11.2.- ANEXO B. ÍNDICE DE TABLAS.

Tabla 3.1.- Grados de criticidad 20
Tabla 5.1.- Periodicidad y Tipo de copia 41
Tabla 5.2.- Secuencia de Respaldo 42
Tabla 5.3.- Soporte físico 43
Tabla 5.4.- Lugar de almacenamiento 44
Tabla 5.5.- Número de copias y versiones activas 45
Tabla 6.- Principales riesgos 55
Tabla 6.1.- Valoración de Incendio en todo el edificio 59
Tabla 6.2.- Valoración de Incendio en parte del edificio 60
Tabla 6.3.- Valoración de Incendio en alguna sala 61
Tabla 6.4.- Valoración de Impacto de un rayo en el edificio 62
Tabla 6.5.- Valoración de corte de electricidad de larga duración 63
Tabla 6.6.- Valoración de corte de electricidad de corta duración 63
Tabla 6.7.- Valoración de Inundación en el edificio 64
Tabla 6.8.- Valoración de Inundación sin daño en el edificio 65
Tabla 6.9.- Valoración de Filtraciones o humedades 66
Tabla 6.10.- Valoración de Seísmo de gran magnitud 67
Tabla 6.11.- Valoración de Seísmo de menor magnitud 68
Tabla 6.12.- Valoración de Temblores sin consecuencias 69
Tabla 6.13.- Valoración de Corte eléctrico por un largo periodo 70
Tabla 6.14.- Valoración de Corte eléctrico por un corto periodo 71
Tabla 6.15.- Valoración de Corte momentáneo de electricidad 71
Tabla 6.16.- Valoración de Cortes de Agua superiores a un día 73
Tabla 6.17.- Valoración de Cortes de Agua inferiores a un día 73
Tabla 6.18.- Valoración de Cortes esporádicos de agua 73
Tabla 6.19.- Valoración de Cortes de telecomunicaciones 75
Tabla 6.20.- Valoración de Cortes de telecomunicaciones por un periodo corto 75
Tabla 6.21.- Valoración de parada momentánea de las telecomunicaciones 76
Tabla 6.22.- Valoración de Sabotaje con importantes daños 77
Tabla 6.23.- Valoración de Sabotaje con diversos daños 78
Tabla 6.24.- Valoración de Sabotaje con daños leves 79

Tabla 6.25.- Valoración de Atentado con impacto grave. 80
Tabla 6.26.- Valoración de Atentado con impacto serio. 81
Tabla 6.27.- Valoración de Atentado con daños leves. 81
Tabla 6.28.- Valoración de Amenaza de bomba con explosión. 83
Tabla 6.29.- Valoración de Amenaza veraz de bomba. 83
Tabla 6.30.- Valoración de Falsa amenaza de bomba. 84
Tabla 6.31.- Valoración de Vandalismo con graves consecuencias. 85
Tabla 6.32.- Valoración de Vandalismo con leves consecuencias. 86
Tabla 6.33.- Valoración de Vandalismo con personal en el exterior. 86
Tabla 6.34.- Valoración de Huelga de larga duración. 88
Tabla 6.35.- Valoración de Huelga de corta duración. 88
Tabla 6.36.- Valoración de Huelga de un día de duración 89
Tabla 6.37.- Valoración de Errores que afecten seriamente 90
Tabla 6.38.- Valoración de Errores que afecten levemente 91
Tabla 6.39.- Valoración de Errores sin relevancia 91
Tabla 6.40.- Valoración de Errores de mantenimiento en los servidores 93
Tabla 6.41.- Valoración de Errores de mantenimiento en los terminales 93
Tabla 6.42.- Valoración de Errores de mantenimiento en las aplicaciones 94
Tabla 6.43.- Valoración de Errores que produzcan daños graves 95
Tabla 6.44.- Valoración de Errores que produzcan daños leves 95
Tabla 6.45.- Valoración de Errores sin efectos 96
Tabla 6.46.- Valoración de Errores de explotación graves 97
Tabla 6.47.- Valoración de Errores de explotación leves 98
Tabla 6.48.- Valoración de Errores de explotación graves 98
Tabla 6.49.- Valoración de Ausencia de un número considerable de personas 100
Tabla 6.50.- Valoración de Ausencia de un número medio de personas 100
Tabla 6.51.- Valoración de Ausencia de un número mínimo de personas 101
Tabla 6.52.- Valoración de Robo de servidores y equipos 102
Tabla 6.53.- Valoración de Robo de una cantidad considerable de equipos 103
Tabla 6.54.- Valoración de Robo de algún equipo 103
Tabla 6.55.- Valoración de Robo de copias de respaldo 104
Tabla 6.56.- Valoración de Robo de información vital 105
Tabla 6.57.- Valoración de Robo de información poco relevante 105

Tabla 6.58.- Valoración de fallo grave en los servidores 107
Tabla 6.59.- Valoración de fallo en diversos terminales 107
Tabla 6.60.- Valoración de fallo leve en algún terminal 108
Tabla 6.61.- Valoración de Ataque de virus grave 109
Tabla 6.62.- Valoración de Ataque de virus con daños localizados.....110
Tabla 6.63.- Valoración de Ataque de virus leve 110
Tabla 8.1.- Planificación del proyecto.....147
Tabla 11.1.- Horas empleadas para desarrollar el proyecto 156

11.3.- ANEXO C. ÍNDICE DE FIGURAS.

Figura 1.1.-Plan general de seguridad 4
Figura 2.1.- Organigrama de la empresa 8
Figura 2.2.- Topología de Red.....15
Figura 3.1.- Aplicaciones Críticas 22
Figura 6.1.- Componentes de riesgo.....52
Figura 7.1.- Esquema de funcionamiento del CAU.....137