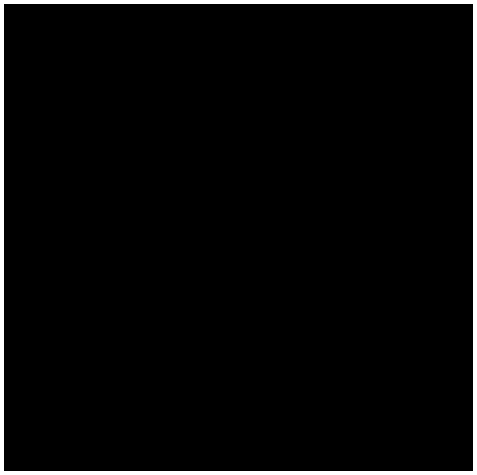
ESCUELA POLITECNICA DEL EJÉRCITO

SEDE LATACUNGA



FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

TEMA: PLAN MAESTRO DE RECUPERACIÓN Y FORTALECIMIENTO EN SEGURIDAD DE LA INFORMACIÓN PARA OMNES LTD.

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS E INFORMATICA

ELABORADO POR: WALTER EDUARDO ORTIZ MAZA

DIRECTOR: ING. JACHO, NANCY

CODIRECTOR: ING. ESPINOZA, EDISON

LATACUNGA, 2003

CONTENIDO

Pág.

I.- SEGURIDAD DE LA INFORMACION

1.1. INTRODUCCIÓN

En este capitulo, se determinara el marco teórico a seguir para el desarrollo del proyecto, es importante determinar las bases teóricas, base fundamental para el desarrollo de cualquier proyecto que se desea realizar, conocimientos teóricos que permitirán encaminar esfuerzos para el alcance de los objetivos planteados inicialmente.

En la actualidad no es suficiente que la empresa se restringa a los campos de higiene y seguridad de trabajo o adquiera una póliza de seguros, como ha sido costumbre. En lugar de soluciones parciales y aisladas, ahora se tiene que buscar soluciones integrales y óptimas para lograr mayor eficiencia dentro de la empresa y prevenir riesgos.

Nos hemos referido hasta aquí a la empresa, no sólo a la infraestructura de EDP. Esto se debe a que la empresa es el súper conjunto del centro de cómputo. El procesamiento de datos es una función de apoyo al negocio. Por lo tanto, cualquier tipo de amenaza a la seguridad de la empresa (o cualquier tipo de organización) lo es también para la seguridad de las instalaciones de cómputo.

1.2. ¿QUES ES LA INFORMACION?

Información es una palabra usada de muchas maneras, pero en relación con el procesamiento electrónico de datos (EDP por sus siglas en ingles), significa "datos recopilados y presentados de modo que contengan un significado”.

Un sistema efectivo de información basado en EDP que puede producir información correcta para la persona indicada en el tiempo necesario, apoyando (o habilitando) la toma de decisiones correctas, se ha vuelto uno de los factores competitivos más importantes en estos días.

En términos genéricos, el objetivo de proteger la información apunta a obtener:

- Confidencialidad, que los mensajes transferidos o recibidos sean secretos y nadie más que su legítimo destinatario tenga acceso a ellos.

- Disponibilidad, que los recursos estén disponibles cuando se necesiten, y que no se usen indebidamente o sin autorización de su autor.
- Integridad y confiabilidad, que consiste en la certeza que el mensaje transferido no ha sido modificado en ninguna parte del circuito o proceso de transferencia.

Al ser la información un parte fundamental para instituciones públicas y privadas es necesario tener seguridad.

1.3 NIVELES DE SEGURIDAD

En el tema de seguridad de los datos se distinguen tres niveles:

1. Seguridad a nivel de los sistemas.
2. Seguridad en recursos y servicios.
3. Seguridad de la información.

1.3.1. Seguridad a Nivel de los Sistemas

En el nivel de los sistemas, el administrador tiene la opción de arbitrar las siguientes medidas de seguridad:

- Control de contraseñas (*passwords*) o claves secretas de usuarios. Implica identificar contraseñas triviales o fáciles de detectar; manejar un sistema de contraseñas con tiempo de expiración, y detectar cuentas sin contraseñas que generen alarmas ante fallas reiteradas de acceso.
- Control de usuarios; es decir, revisión periódica de las características del usuario en relación con los privilegios otorgados, acceso a información disponible, horario de conexión asignado, etc.
- Control de acceso. Implica revisar periódicamente cómo, cuándo y desde dónde se puede acceder al sistema.
- Generación de informes que den cuenta de anomalías o problemas encontrados en cualquiera de los controles indicados anteriormente.

1.3.2. Seguridad a nivel de recursos y servicios

Las medidas de seguridad orientadas a proteger la red misma y los recursos y servicios involucrados, como ancho de banda, tiempo de respuesta, acceso a servidores de la red, etc., consisten en la instalación de mecanismos o dispositivos denominados cortafuegos (*firewalls)*, cuya función principal es mantener un control del acceso a la red y a los recursos.

1.3.3. Seguridad de la información

El nivel de seguridad de la información es probablemente el más importante, pues es aquél donde más participa el usuario y al igual que en los casos anteriores distingue varias clases y niveles:

A nivel de protocolos, el IP provee dos encabezamientos (header) de datagramas, destinados a la seguridad: el AH (Authentication Header) y el ESP (Encapsulating Security Payload), cuyos detalles pueden encontrarse en el RFC 1825, Security Architecture for IP.

A nivel de transporte, Netscape propuso el estándar SSL (Secure Socket Layer), que genera un túnel virtual entre el cliente y el servidor, a través del cual circulan los datos encriptados con el sistema DES, en condiciones de seguridad.

La información y los sistemas de información son muy valiosos. Por lo tanto deberían, ser tratados como un recurso estratégico, estos deberían ser protegidos para asegurar la credibilidad junto con la calidad y precisión al usuario, el responsable de la seguridad de la información es el “propietario” de la misma.

El principal desafío (y riesgo) para la seguridad está representado no por la tecnología sino por la gente involucrada. Por lo tanto, es necesario decidir qué información no debería estar disponible para todos, pero si para cierto personal que tenga autorización para ello.

1.3.4. Objetivos de la seguridad de la información

Los Objetivos principales son:

- Mejorar la seguridad y salvaguardar el personal y demás recursos de la empresa.

- Prevenir los desastres, a través de la reducción de los riesgos.
- Asegurar los preparativos para atender las emergencias.

1.4. FACTORES PARA MANTENER SEGURIDAD DE LA INFORMACIÓN

Toda compañía debe realizar un monitoreo de su entorno en las ultimas dos década los cambios se han venido presentando de una manera acelerada para lo cual una organización debe prepararse para soportar o prevenir dichos cambios, la mayoría de las organizaciones no utilizan dicha información recogida para desarrollar alternativas. Existe el modelo de planeación estratégica que exige a una organización monitorear su entorno no existe un principio y un fin de una planeación estratégica es un modelo que debe estar en constante desarrollo, este modelo otorga información al equipo de planeación y a la organización sobre lo que está sucediendo y la posibilidad de lo que pueda suceder algo que puede afectar a las operaciones normales de la empresa. La organización que monitorea los grandes cambios sociales e integran su impacto en el proceso de planeación obviamente posee una ventaja competitiva sobre otras empresas para una planeación debe considerarse los siguientes aspectos:

Económico: porque la empresa cuando madura ve surgir el ciclo de negocios es probable que comience a pensar en la expansión una meta importante de la planeación estratégica consisten en mantenerse dentro de la situación expansión/contracción y evitar las situaciones de expansión excesiva y supervivencia.

Aspectos Tecnológicos: La influencia de los cambios en los aspectos tecnológicos es profundo e importante, aunque habría una variación en el grado hasta el cual una organización se viera inhabilitada por dicha tecnología rara vez dejara de verse afectada.

Aspectos Políticos: Los aspectos más importantes son los cambios en la regulación gubernamental, simultáneamente con un aumento de la preocupación del gobierno por el daño físico, el cambio constante de las políticas tributarias que afecta a las políticas organizacionales como la incursión a la investigación y el desarrollo.

Aspectos Sociales: Son los grandes cambios en la sociedad que ocurren en el paso del tiempo, que afectan directamente la forma como funcionan las organizaciones a como deben operar.

1.4.1. Factores Externos

Entre los factores externos a la empresa, los desastres representan uno de los riesgos más fuertes. La existencia de este riesgo es una de las razones por las que deben desarrollarse planes de contingencia y aplicarse medidas en pro de la seguridad de la información.

Presentamos ahora la clasificación de calamidades utilizada en las bases para el Establecimiento del Sistema Nacional de Protección Civil.

Este esquema de clasificación se elaboró con base en algunas características de las calamidades, como el análisis de sus procesos de producción y generación, se postula cuatro tipos de fenómenos, y son los siguientes:

1. Calamidades de origen hidrometeorológico: lluvias, tormentas de granizo, inundaciones, temperaturas extremas, sequías, tormentas eléctricas, vientos.
2. Calamidades de origen químico: contaminantes, envenenamientos, incendios, explosiones, radiaciones, calamidades de origen sanitario, epidemias, plagas.
3. Calamidades de origen socio-organizativo: explosión demográfica, fallas humanas, disturbios sociales, actos delictivos, accidentes, acciones bélicas, drogadicción-alcoholismo.
4. Efectos negativos producidos por la operación actual de servicios: interrupción de servicios.

Las calamidades listadas anteriormente pueden presentarse en todo el territorio nacional, en lo que respecta a fenómenos destructivos y desastres, la Ciudad de Quito es muy vulnerable a este tipo de eventos por la alta Propensión que presenta a diversos tipos de siniestros.

Además de eso, en los últimos años se ha registrado un aumento considerable en la incidencia de desastres naturales a nivel mundial, los cuales también han aumentado en intensidad, y la causa principal, ha sido la acción del hombre, sus contaminantes, la destrucción de habitas naturales, etc. Los científicos piensan que esto generará en los próximos años (o tal vez ya haya comenzado) un gran cambio climático como los que han ocurrido en la historia del planeta. Este cambio producirá una ocurrencia inusual de desastres naturales (como la que se ha observado), por su cantidad y gravedad, a nivel de todo el globo terráqueo y eventualmente afectarían a las ciudades ya mencionadas y al capital e intereses económicos de la Empresa.

TABLA 1.1.

Posibles Amenazas externas a Centros, Equipos y Sistemas de Cómputo

Accidentes aéreos	Accidentes nucleares
Amenazas de bomba	(Evacuación)
Comida tóxica	Alto índice de criminalidad
Fallas en controles de medio	Clima gélido
ambiente	Guerra
Fuego	Derrames químicos
Inundaciones	Desórdenes civiles
Tormentas de hielo	Disturbios por construcciones
Volcanes	Terremotos
Terrorismo	Tormentas de arena
Accidentes	Tormentas de nieve

1.4.2. Factores Internos

Hemos mencionado con anterioridad cuáles son los riesgos a los que está expuesta la empresa, y por ende a los que se exponen los sistemas de información como parte integrante del gran sistema.

Las contingencias que pueden afectar a los sistemas de información y en general a los componentes de la tecnología de información que soporta la

operación de la mayoría de las empresas y organizaciones hoy en día (ver Figura 1.1)

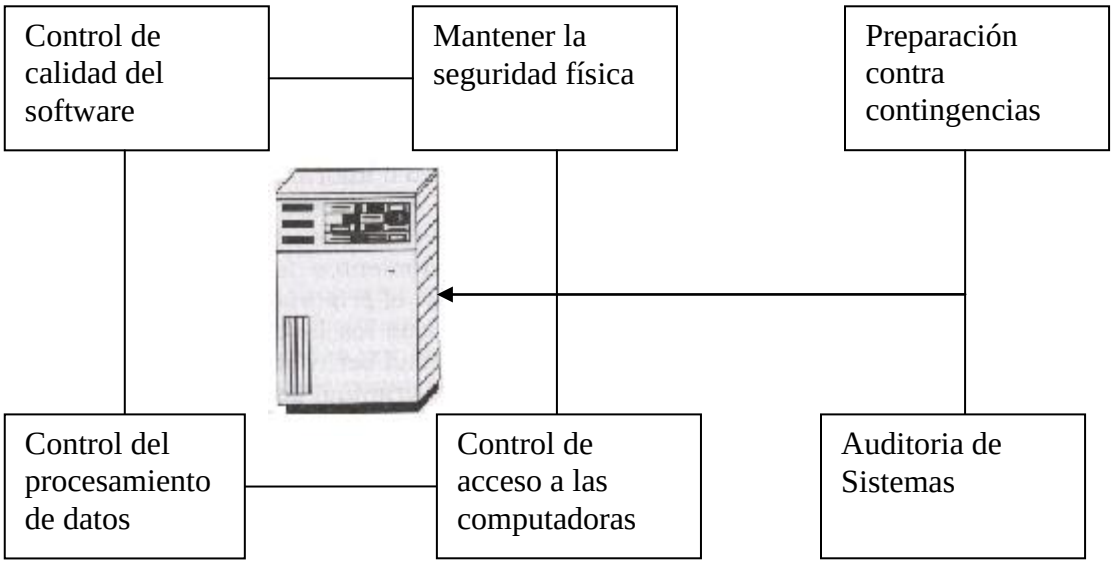


Figura 1.1 Minimizando Accidentes y Crimen por Computadora

La tecnología de la información ha cobrado gran importancia en la actualidad. Es decir, el colapso de los sistemas de información (por mencionar un ejemplo), puede llevar a una situación de grave crisis a cualquier organización que ha adquirido un cierto grado de dependencia en dichos sistemas.

Existen muchos peligros que pueden provocar serías consecuencias internas a las operaciones del centro de cómputo. Ver Tabla 1.3.

TABLA 1.3: Posibles peligros que provocan consecuencias a centros, equipos y sistemas de cómputo.

Abuso de alcohol	Embargos
Acceso reducido u obstruido	Errores de programación
Agua	Espionaje industrial
Clima cálido extremo	Explosiones por fugas de gas
Demostraciones de nuevos equipos	Falta de inversión
	Fluctuaciones eléctricas
Desfalcos	Paros laborales/huelgas
Disputas de empleados	Sabotajes

Descuido humano
error de "dedo"
error del operador
Montar volumen equivocado
Usar versión, de programa equivocado
Daño físico al disco o la cinta.
Abuso de drogas
Calor y /o humedad
Empleados disgustados
Errores u omisiones en datos
Evacuación de áreas de trabajo
Falla en comunicaciones
Fallas de software
Fallas en hardware
Falta de supresores de incendio
Interrupción de fluido eléctrica
Robos
Virus en computadoras
Crimen por computadora
Empleados vendiendo información

1.4.3. Condiciones que Incrementan la Vulnerabilidad

Se han presentado una serie de contingencias relacionadas con los sistemas. Para desarrollar medidas efectivas de seguridad contra estos riesgos, es necesario entender bien sus causas. Aunque cada desastre implica una situación particular, es posible identificar condiciones que incrementa la vulnerabilidad a cada tipo de contingencia, o a varios tipos de éstas (ver Tabla 1.4)

TABLA 1.4: Condiciones que Incrementan la Vulnerabilidad a Desastres

	CONTINGENCIA	**CONDICIONES QUE INCREMENTAN LA VULNERABILIDAD**
Desastres no Intencionales	Error del operador	Dificultad para prever cómo funcionarán los sistemas y como se adaptarán a ellos los usuarios
		Complacencia al suponer que el sistema operará como se espera.
		Falta de trabajo y cuidado para asegurar que los funcionen correctamente.
	Falla de hardware	No creer que el hardware pueda fallar.
		Dificultad para decir si la falta está en el hardware o en el sistema.

	CONTINGENCIA	CONDICIONES QUE INCREMENTAN LA VULNERABILIDAD
	Errores de Software	Diseño y pruebas inadecuadas.
		Factores no esperados que afectan la operación del sistema.
	Errores en los datos	Fallas en los procedimientos
		Falta de capacidad en el software para detectar muchos tipos de errores.
		Falta de cuidado
		Respaldos no adecuados.
	Daño a las Instalaciones y medios de almacenamiento	Seguridad física contra fenómenos naturales no adecuada.
		Protección no adecuada contra fallas en los sistemas de apoyo a la computadora
		Mal Diseño
	Desempeño no adecuado de los sistemas.	Demanda de trabajo no prevista.
Desastres intencionales	Robo	Diseño no adecuado del sistema de cómputo.
		Existencia de muchos objetivos fáciles para el robo
		Sistemas distribuidos.
	Vandalismo y Sabotaje	Prevención no adecuada de accesos no autorizados a sistemas e instalaciones
		Procedimientos no adecuados de seguridad en toda la empresa.

En forma general, la información computarizada es particularmente vulnerable porque:

- Está más concentrada. Una computadora, o algunas veces una base de datos/grupo de archivos, puede almacenar o contener información de

muchos departamentos, los cuales fueron anteriormente guardados en kardex individuales en diversas áreas.

- Es más accesible. En el pasado, solamente unos pocos empleados tenían acceso a sus archivos. Hoy en día, miles de empleados usan computadoras y, a menos que se hayan tomado medidas apropiadas de seguridad de acceso a la información confidencial, ésta podrá ser fácilmente accedida.
- Está sujeta a daños no detectables o uso indebido. No es posible ver físicamente los datos almacenados en una computadora, así, los cambios y eliminaciones no deseadas son menos obvias. Un solo error puede dañar o eliminar un archivo, y un comando puede borrar todos los archivos contenidos en un disco duro.

1.5. SEGURIDAD FISICA

1.5.1. Antecedentes

Mantener la seguridad física es un primer paso que resulta casi obvio, para proteger las instalaciones de cómputo y comunicaciones. Podemos definirla básicamente como un conjunto de lineamientos y procedimientos cuyo objetivo es evitar o disminuir la exposición a riesgos ya sean internos o externos en las instalaciones físicas de cómputo. Las medidas de seguridad física deben tomar en cuenta riesgos, como accidentes, desastres naturales, ataque por intrusos, condiciones ambientales, etc.

1.5.2. Desastres Naturales y de Origen Mixto (Calamidades)

Los desastres naturales se los considera calamidades cuando estos ocasionan daño a la empresa, el centro de procesamiento de datos “Centro de Computo”, para lo cual debemos prever, identificarlos y determinar hasta que grado podemos mitigarlos, las calamidades de origen mixto son producidos en combinación por el hombre y la naturaleza para lo cual se deberá instruir al personal tanto ajeno como de la empresa de las normas de seguridad que adopte la empresa.

Incendios: Los incendios son definidos como la ignición no controlada de materiales inflamables y explosivos, dado el uso inadecuado de combustibles,

fallas en instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. Los daños que produce un incendio son generados por el fuego, el calor, los productos de la combustión, el agente extinguidor y tienen como consecuencia destrucción de construcciones y estructuras. Los incendios son comúnmente considerados como el principal y más temido riesgo en instalaciones de cómputo; sin embargo, estadísticamente el agua es la causa del mayor número de desastres en instalaciones de cómputo. De acuerdo a la *National Fire Protection Assodation (NFPA),* el costo promedio de un incendio en un centro de procesamiento de datos en 1984 fue de USD 2.6 millones.

Inundaciones: Se considera inundación al flujo o a la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por la falta o insuficiencia de drenaje tanto natural como artificial. Según la Oficina de Servicios de Soporte a Seguros de la Agencia Federal de Manejo de Emergencias, los pagos hechos a poseedores de pólizas de seguros contra inundación, alcanzaron los USD 72 millones en 1986. Entre las causas comunes de inundaciones están: fugas de tuberías de agua, aire acondicionado (fugas de agua o condensación), sistemas de enfriamiento por agua (así se enfrían algunos equipos computacionales), rociadores, etc.

Falla de la Corriente Eléctrica: Las consecuencias de una interrupción en el suministro de electricidad son proporcionales al grado de dependencia en la computadora, esto implica dependiendo de la cantidad de procesamiento de datos exista, será mayor ó menor el grado de perdidas económicas, la falta del suministro eléctrico se lo puede mitigar mediante la instalación de fuentes de energía alternas ya sea mediante la utilización de UPS, o mediante la instalación de plantas de Energía Eléctrica.

Falla en el Sistema de Aire Acondicionado: Este sistema controla la temperatura y humedad y puede proporcionar filtración de aire. Una falla en este sistema causa un paro inmediato de el procesamiento, ya que la temperatura aumenta rápidamente porque las computadoras, y en especial dispositivos como

unidades de disco y cinta (que contienen motores), que generan grandes cantidades de calor.

Contaminación: Una importante, pero frecuentemente desapercibida causa de incendio, es la contaminación ambiental. La entrada de partículas contaminantes al equipo electrónico, puede causar corto circuitos e incluso iniciar incendios en equipo de procesamiento de datos. Surge la pregunta: ¿cómo se introducen los contaminantes al ambiente supuestamente limpio del centro de cómputo? Mientras que ciertos contaminantes son introducidos por los operadores (incluyendo fibra de ropa, partículas de cabello, piel, ceniza, etc.), la mayoría de las partículas son traídas por el aire y transportadas dentro de los equipos sensibles a través de las entradas de aire debajo del piso falso. Algunos de los contaminantes más comunes son; polvo de cemento, yeso y tierra, contaminación "urbana", y partículas metálicas (conductoras de electricidad). Muchos contaminantes pueden absorber humedad además de conducir electricidad.

1.5.3. Acciones Deliberadas

Son acciones voluntarias por individuos ajenos o propiamente por la empresa cuyo único fin es perjudicar a un bien común de una forma total o parcial, denigrando la continuidad en el negocio para lo cual la empresa debe prever acciones para mitigar y prevenir accidentes que vayan en contra de los intereses de la empresa.

Robo de Equipos e Información: En los centros de cómputo se encuentran activos son de gran valor monetario, que resultan susceptibles de ser sustraídos. Más grave aún puede resultar la sustracción de información (parte de la cual tiene carácter de confidencialidad), para lo cual deberá tener políticas y procedimientos de entrada y salida de equipos (hardware) de la compañía, contar con medios electrónicos y personal de seguridad que restringa y prevenga la salida involuntaria de equipos.

Actos Destructivos Premeditados: Son los actos terroristas de los cuáles nuestro país ha estado prácticamente exento, pero no por eso podemos decir que sea inmune, sin embargo debido a la situación que vive nuestro vecino país Colombia debido al conocido plan Colombia que nos hemos visto afectados de

una manera indirecta con la sobrevenida de colombianos a nuestro territorio, y la sobrevenida de problemas sociales que afectarían de manera indirecta a la empresa, para lo cual la empresa no se vea afectada se debe tomar las medidas precautelares que amerita ésta situación.

Amenazas de los Vecinos: La actividad que se desarrolla en la zona circundante puede crear un riesgo para el procesamiento de la información en cualquier empresa. La cercanía de aeropuertos, carreteras muy transitadas, obras en construcción o empresas que manejan productos químicos o explosivos, aumentan considerablemente el riesgo y deben ser tomadas en cuenta en los de seguridad general y de contingencia, así como en el análisis de riesgo. Lo mismo ocurre cuando el centro de procesamiento de datos está ubicado en una zona de alta criminalidad o en áreas de gran propensión a desastres naturales o con gran interferencia electromagnética. Asimismo, en las áreas adyacentes a los sitios industriales o a grandes complejos de oficinas, las variaciones de voltaje en el suministro de energía eléctrica son un problema frecuente.

1.5.4. Control del Medio Ambiente

Controlar la variabilidad del medio ambiente nos permitirá prevenir de situaciones insospechables, situaciones que perjudicarían a los equipos de computo, que es nuestra prioridad prevenir de acciones de cualquier índole que puedan detener su normal funcionamiento, al tener un control nos permitirá conocer situaciones extremas, y soportables por los equipos, esto permitirá evitar de una rápida degradación de los equipos de computo de la empresa, tomando medidas precautelares.

Humedad: La humedad afecta no sólo a los equipos sino también a las cintas, discos y papel por esa razón se deben instalar sistemas de detección de fugas de líquidos. No deben pasar tuberías por encima ni debajo ni a los lados directamente del centro de cómputo, almacenes de cintas, discos, papel, etc. Se debe tener cuidado con fugas de agua de equipos enfriados por este liquido y fugas de los aparatos de aire acondicionado.

Temperatura: Las instalaciones de cómputo son muy sensibles a la temperatura, incluso temperaturas de 50 a 60^{O} C Pueden tener efectos muy

dañinos en equipos y medios de almacenamiento de información (ver Tabla 1.5). Por lo tanto deben existir sistemas de aire acondicionado con salidas bien distribuidas, también la construcción del centro de cómputo tiene que estar bien diseñada de modo que no haya fugas del aire frío ni entradas de aire caliente (no debe tener ventanas al exterior), polvo o luz solar. En todas las instalaciones existen grandes problemas con el aire acondicionado, ya que éste implica un doble riesgo: (1) las fluctuaciones o la descompostura del sistema de aire condicionado, puede ocasionar que la computadora tenga que ser apagada y (2) las instalaciones de aire acondicionado, son una fuente de incendios frecuente y también son susceptibles a la intrusión física especialmente a través de los ductos. Para poder afrontar estos riesgos se requiere lo siguiente; l) instalar equipos de aire acondicionado de respaldo donde se hayan establecido los sistemas principales, (2) instalar redes de protección en todo el sistema de ductos y (3) instalar detectores de incendios en los ductos.

TABLA 1.5: Temperaturas a las que Empiezan a Ocurrir Daños

Equipo de cómputo	79º C
Cintas magnéticas/disquetes	38-50º C
Discos	65º C
Papel/tarjetas perforadas	176º C
Microfilm. / micro fichas	107º C (con vapor), 149º C (sin vapor)

Aun en caso de incendio, las cintas magnéticas pueden ser salvadas en ocasiones. Durante un incendio, las cintas magnéticas se comportan en forma similar a un rollo de papel bien apretado, es decir resisten prenderse debido a la falta de oxígeno. El problema es que después de temperaturas relativamente bajas, la información se empieza a distorsionar. Un daño mayor puede ser causado por el vapor, que puede ocasionar que las capas de la cinta se peguen.

Limpieza: Resulta vital mantener limpio el centro de cómputo. También es importante para la estabilidad de la operación, que el aire esté limpio y libre de partículas (se deben instalar filtros). Otras medidas que se pueden poner en práctica para eliminar ciertos tipos de contaminación y para minimizar el impacto de contaminantes que no pueden ser totalmente eliminados son las siguientes:

- prohibir comer, fumar y beber dentro del centro de cómputo
- vaciar los basureros y sacar el papel de desperdicio del centro de cómputo
- poner las impresoras fuera del cuarto donde están las CPU, unidades de cinta, etc.
- observar medidas apropiadas de mantenimiento del piso falso, etc.
- asegurar que todas las computadoras estén equipadas con los mejores filtros que el vendedor puede proveer
- no instalar purificadores de aire generadores de iones y dar un buen mantenimiento al aire acondicionado

1.5.5. Control de Acceso al Centro de Cómputo (Medidas de Prevención y Mitigación)

Este tipo de sistemas garantizan que sólo el personal autorizado podrá ingresar al CPD (Centro de Procesamiento de Datos), con lo cual se disminuirá considerablemente el riesgo de robo, destrucción o manipulación no autorizada de equipos e información (desastres producidos por el hombre). Los controles durante los descansos y cambios de turno son de especial importancia. El medio que permite identificar al personal, puede ser a través de teclados y claves numéricas, otros realizan la identificación mediante lectores de tarjetas codificadas o tarjetas con cintas magnéticas, otros más lo hacen con una combinación de los sistemas anteriores. Hay otros sistemas de identificación que se basan en quién es la persona y no en qué tiene la persona |que acabamos de mencionar |, como los de reconocimiento de firmas, de huellas digitales, sistemas de reconocimiento de las líneas de la mano, de voz, reconocimiento de la retina, etc., llamados sistemas biométricos. A los sistemas descritos anteriormente se les llama "sistemas de identificación y autentificación", ya que intentan no sólo conocer la identidad del usuario, sino de saber si esa identidad es auténtica. Cuando se utilicen estos sistemas automáticos para las puertas, debe existir una puerta adicional que se usa como salida de emergencia. Las aperturas que se usen para recepción y entrega de datos deberían estar en una área separada del centro de cómputo con una división a prueba de fuego.

Tomando en cuenta que el centro de cómputo está (en la mayoría de los casos) dentro del edificio de oficinas de la empresa, las medidas de control de acceso al centro de cómputo comienzan con las medidas de control de acceso al edificio.

El Diseño de la Construcción: Para planear la instalación de un centro de cómputo deben intervenir desde el principio los especialistas de las áreas de informática, inmuebles o construcciones, organización y de seguridad, de tal manera que se encuentre un equilibrio entre la magnitud del equipo y sus operaciones, el valor o confidencialidad de la información que procesará así como las pérdidas en caso de suspensión de operaciones, la disponibilidad de espacios o terrenos, los recursos económicos disponibles y la capacidad técnica y de recursos humanos del área de seguridad. Las rutas de accesibilidad al centro de cómputo tienen que ser limitadas, no debe tener muros exteriores ni ventanas etc.

Ubicación del Centro de Cómputo: El centro de cómputo no debe situarse en sótanos ni planta baja, tampoco en el último piso del edificio (sobre todo en un edificio alto) ya que está más expuesto a choques de aeronaves, etc. También debería evitarse instalar centros de procesamiento electrónico de datos en zonas con fallas geológicas. En general, son preferibles zonas sub-urbanas para instalar centros de cómputo, y éstos deben encontrarse por lo menos a 60 metros de distancia del acceso público más cercano. No deben estar junto a áreas públicas tales como centros comerciales (por riesgo de bombas), estacionamientos (por riesgo de auto-bombas) o restaurantes (por riesgo de explosiones en las cocinas).

Barreras de Protección: Básicamente hay cuatro niveles jerárquicos:

a) Protección perimetral: los controles ubicados en el área externa del predio y que lo limitan con las colindancias inmediatas, Ej. bardas, rejas, puertas de acceso, casetas de vigilancia, etc.

b) Protección, de inmueble: se consideran los controles ubicados en la periferia del edificio mismo (de la construcción), Ej. muros de material fuerte, puertas, etc.

c) Protección del área: se logra con la sectorización. que consiste en el agrupamiento de las áreas por funciones, de tal manera que no existan cruces de personal ni de información entre las mismas. Con esto se

obtiene una distribución racional de los recursos de seguridad con que se cuente. Deben vigilarse las entradas normales al área y otras como ductos de aire acondicionado, etc., con sistemas de alarma, sistemas electromecánicos de detección de intrusos, etc.

Protección de objeto: esta última barrera nos permite diseñar la protección de áreas específicas que por su importancia o valor requieren de un tratamiento especial, Ej mantraps, sistemas sofisticados de detección de intrusos como sistemas fotométricos, sistemas de detección de movimiento por sonido, ultrasonido o microondas, sistemas de detección de ruido y vibración (acústicos y sísmicos), sistemas de proximidad, detectores de metales en las entradas, etc.

Guardias y Monitoreo Electrónico: Se emplean policías que permanecen constantemente a la entrada del centro de cómputo vigilando o al menos haciendo rondas cada determinado tiempo o monitoreo a través de un circuito cerrado de televisión.

Procedimientos Administrativos: Se utilizan gafetes de identificación, listas de acceso a áreas restringidas, etc., con el objetivo de restringir el acceso no autorizado de personal que innecesariamente tendría nada que realizar en dichas áreas ó lugares.

Control de Acceso de Terceras Personas: Aquí se incluye al personal de limpieza, a los técnicos de los diversos sistemas localizados en el centro de cómputo (Ej. aire acondicionado, impresoras) y a los visitantes (autorizados). Todos ellos deben ser identificados plenamente y controlados y vigilados en sus actividades durante el acceso.

Sistemas Biométricos: Cinco tecnologías biométricas son las que se están comercializando principalmente: patrón de huellas digitales, geometría de la mano, "scaneo" retinal, verificación de voz, y dinámica de firmas, que a continuación revisaremos brevemente. La necesidad de un buen sistema de identificación es por lo que muchos consumidores compran sistemas biométricos, pero éstos no pueden ser cien por ciento exactos todo el tiempo. Existen dos tipos de errores (que están inversamente relacionados): (1) el dispositivo biométrico

rechaza a una persona cuya identidad es valida y (2) la frecuencia con que el dispositivo acepta aun impostor.

Patrón de Huellas Digitales: Es una técnica de identificación personal con la que estamos muy familiarizados, por lo que el mercado .rápidamente la aceptó. Hay dos tecnologías: comparación de patrones y comparación de minutas, siendo esta última la de mayor credibilidad porque es la que usa la Oficina Federal de Investigaciones de los Estados Unidos (FBI).

Geometría de la Mano: Estos sistemas miden, graban y comparan longitud de dedos, translucidez de la piel, grosor de la mano o forma de la palma.

"Scaneo" Retinal: Los patrones de Venas en el ojo humano son únicos. Un scanner retinal analiza esas venas para determinar la identidad de una persona. Esta tecnología, introducida en 1983, se usa principalmente en instalaciones de alta seguridad. Muchos consumidores estaban preocupados acerca de contraer gérmenes, pero ahora los scanners de retina no requieren contacto.

Verificación de voz: Esta técnica se desarrolló a principios de la década de 1970. Los primeros sistemas tenían tasas de error muy altos, por ejemplo, un resfriado podía alterar la voz y dejar a un usuario autorizado sin posibilidad de ser aceptado. Afortunadamente esto se ha corregido casi en su totalidad.

Dinámica de Firma: Desafortunadamente, los falsificadores son muy hábiles para duplicar firmas. Por esta razón, las firmas estáticas no son útiles como identificación personal. Las técnicas más nuevas se basan en un censado electrónico y medición de los movimientos de la pluma mientras se está firmando. La falsificación de este tipo de firma es casi imposible. Estos sistemas ahora se basan en un tapete sensible, donde se firma. Debido al tiempo extra y el esfuerzo para firmar, este método no es un buen candidato para control de acceso físico a áreas con alto volumen de tráfico, especialmente donde las mismas personas están entrando y saliendo todo el día. Su aplicación para control de acceso es más adecuada para terminales o entradas a instalaciones de alta seguridad.

Sistemas de Protección Contra Intrusos: Estos sistemas permiten detectar la, presencia de personas no autorizadas en el interior del centro de cómputo y activar una alarma. Por lo general se usan en conjunto con los sistemas de control

de acceso de manera que el ingreso de personal autorizado no implique la activación del sistema de alarma. Algunos tipos de sistemas de detección de intrusos son:

- se rompe un circuito eléctrico
- se cierra un circuito eléctrico
- se interrumpe un haz de luz
- se interrumpe un rayo láser
- se rompe un haz ultravioleta
- se rompe un haz infrarrojo
- detector de sonido o vibración
- detector ultrasónico de movimiento
- radar detector de movimiento
- detector de presencia por variación en un campo eléctrico
- detector de robo (poner una etiqueta especial a cintas y otras cosas que se detecta electrónicamente al salir por la puerta)
- circuito cerrado de televisión

1.5.6. Sistema de Protección Contra Descargas Eléctricas

En toda instalación de equipo de cómputo deberá existir una red de pararrayos que garantice que toda descarga eléctrica atmosférica sea derivada a tierra, con esto también se disminuirá el riesgo de incendio. Otros riesgos son los cambios de voltaje. Por lo tanto, deben instalarse supresores de picos, reguladores de voltaje, dispositivos de monitoreo y alarmas. Muchos constructores de equipo recomiendan conectar el CPU y los periféricos a diferentes circuitos para mantenerlos aislados eléctricamente.

1.5.7. Medidas de Prevención de Incendio

Empiezan desde el diseño y construcción del edificio y del centro de cómputo (materiales resistentes al fuego como aluminio, acero, concreto, cerámica, etc.), así como la selección de su ubicación (Ej., las áreas aledañas al centro de cómputo deben estar bien protegidas contra incendios; y no se debe situar en el último piso del edificio). Utilizar muebles de oficina no combustibles (debe ser

metálicos), gabinetes de almacenamiento resistentes al fuego, cajas de seguridad contra incendios (deben satisfacer los estándares mínimos de la Fíre Insurance Association); pegar placas con la descripción (clara y breve] de los procedimientos de emergencia, etc. Son de gran importancia los sistemas de detección de humo (el detector de humo que se elija deben ser capaz de detectar los distintos tipos de gases que desprendan los cuerpos en combustión) y calor, los cuales deben ser posicionados de acuerdo a las corrientes de aire. ya que los conductores de aire condicionado pueden difundir calor o el humo y no permitir que se active el detector. Tienen que instalarse detectores en los gabinetes, ductos de aire condicionado, bajo el piso falso, en el techo, etc. y estar conectados a sistemas de alarma (o directamente al departamento de bomberos), y además deben señalar la ubicación exacta de la fuente. Estos sistemas de detección pueden proveer otras funciones, como abrir salidas de emergencia, cerrar puertas, controlar elevadores, apagar los equipos y ventiladores, etc.

1.6. SEGURIDAD LÓGICA

1.6.1. Definición

La seguridad lógica es tan importante como la física, incluye normas para el control del acceso a los datos/información, a fin de reducir el riesgo de transferencia, modificación, pérdida o divulgación accidental ó intencional de éstos. La seguridad física y la lógica dependen, para el éxito de cada una, de la eficiencia y fortaleza de la otra, algunas de las principales aplicaciones de las medidas de seguridad lógica son:

- Separar los recursos del sistema de otros materiales al que tienen acceso permitido varios usuarios.
- Proteger los datos de un usuario de los de otro.
- Controlar el acceso de lugares remotos.
- Definir y poner niveles de control de acceso.
- Monitorear el sistema para detectar cualquier uso impropio.

1.6.2. Riesgos Debidos a la Amabilidad de los Sistemas (User-Friendly)

Las microcomputadoras y los paquetes de software de uso muy sencillo han provisto con capacidades o conocimientos en computación a personas sin un entrenamiento formal en el área. Algunos ejemplos de tipos de sistemas amigables al usuario que crean preocupaciones de seguridad son los siguientes:

- Sistemas de Compras para Clientes.
- Sistemas de órdenes y Envíos. Un creciente número de organizaciones industriales están desarrollando sistema de intercambio electrónico de datos (EDI).
- Sistemas de Pedidos de Manufactura.
- Sistemas de Transferencia de Dinero y Comercialización de Acciones.

Todos los anteriores tipos de sistemas están diseñados para ser sencillos de usar, y para incrementar la productividad y eficiencia de una organización a través de sistemas flexibles, debe tenerse mucho cuidado con los riesgos generados por aplicaciones que son quizá demasiado "amables" para el usuario y no tienen controles. Por ejemplo, sistemas que diseñan contraseñas muy cortas y fáciles de recordar y que no se cambian en forma regular, sistemas con controles de acceso demasiado débiles, etc. La exposición de la organización a las violaciones de la seguridad de la información depende del tipo de aplicación.

1.6.3. Riesgos Debidos a la Conectividad de los Sistemas

En sistemas multiusuarios convencionales se ponen barreras alrededor de cada usuario, tanto para prevenirlo de interferir con el sistema como con otros usuarios. En el mundo moderno de redes y estaciones de trabajo éste puede no ser el mejor modelo. Esto apunta ahora hacia un nuevo modelo de seguridad. Es mejor pensar en términos de enclaves seguras alrededor de los cuales se garantiza una seguridad estricta. Este modelo de seguridad es aplicable a sistemas distribuidos, en particular a grupos de estaciones de trabajo con servidores de archivos. Estos últimos pueden estar rodeados por una barrera de seguridad dentro de la que hay una seguridad relajada. En verdad es difícil que exista otra forma en la que un

grupo de estaciones de trabajo pueda hacerse seguro, ya que no hay un sistema operativo central.

1.6.4. Privacia de la Información

Los sistemas de procesamiento de datos pueden almacenar grandes cantidades de información acerca de individuos. La información puede ser recopilada de varias fuentes y entonces comparada. Algunas de estas comparaciones podrían ser inofensivas, pero otras no.

¿Cuándo podría considerarse una violación de la privacia de las personas en un ambiente de negocios? Tal vez, siempre que la información que ha sido recopilada para un propósito y sea revelada a externos para otro propósito, esto se produciría cuando las políticas de seguridad de la información son insuficientes, que permitirían accesos no autorizados, violaciones de la privacia personal e incluso crimen por computadora. Existe un factor adicional que viene a complicar esto: ¿de quién es la información?, ¿del usuario, del área de sistemas?, ó ¿de la Empresa?, es decir, el problema de la "propiedad" de la información.

1.6.5. Integridad de la Información

El término "integridad" se usa para referirse al problema de asegurar la corrección de la información (cobra una relevancia especial en el mundo de las Bases de Datos). Los valores en un banco de datos se pueden volver inválidos de varias maneras. Probablemente la causa más común es una entrada de datos o una actualización en la cual algunos valores son especificados incorrectamente. Este aspecto del problema de integridad a veces se denomina integridad semántica. Los datos también pueden invalidarse como resultado de dos o más modificaciones que individualmente operan correctamente, pero cuya interacción produce resultados inválidos. El término control de concurrencia se usa para describir este problema. Una tercera causa de violación de integridad son las malas funciones de hardware o software.

Confiabilidad del Personal: El mayor daño que puede sufrir un centro de cómputo es el que se hace desde dentro; ni siquiera las fortalezas o los equipos más sofisticados y costosos pueden contra la deslealtad, la deshonestidad o la

negligencia del personal. Los empleados descontentos, o los que recientemente han sido corridos de la compañía representan un riesgo mayor. Por lo tanto, la selección de personal es parte importantísima del esquema integral de seguridad.

Riesgos de Falla del Equipo de Cómputo: Aunque la confiabilidad de los equipos de cómputo está mejorando día con día, estos aún fallan con cierta frecuencia. Hasta una falla en un pequeñísimo componente de una computadora puede ser desastrosa. Esta categoría de riesgo incluye los siguientes peligros:

1. Falla en el CPU
2. Falla en los Dispositivos Periféricos
3. Error del Operador
4. Errores en el Software
5. Errores en los Datos
6. Desempeño Inadecuado de los Sistemas
7. Responsabilidad por Fallas en los Sistemas
8. Piratería de Software
9. Crimen por Computadora Podemos distinguir 2 tipos de crimen por computadora:
    a. Incidentes donde las computadoras se usan para cometer el crimen, .Ej. fraude, desfalco, etc.
    b. Incidentes donde las computadoras o los medios de almacenamiento de información son los objetivos, Ej. instalación de bombas lógicas, intercepción de información, copia no autorizada, etc.
10. Sabotaje
11. Espionaje Industrial
12. Legislación de Crimen por Computadora
13. Emanación Electromagnética
14. Pulso Electromagnético (EMP)
15. Acarreo Electrónico

TABLA 1.6: Ocupaciones de los Ofensores en un Estudio sobre Mal Uso de Computadoras

Factores principales	%
Programadores de aplicaciones	18%
Oficinistas	14%
Otros usuarios de los sistemas	14%
Estudiantes	12%
Administradores	11%
Analistas de sistemas	6%
Operadores	6%
Altos ejecutivos	6%
Otros miembros del área de sistemas	4%
Capturistas	3%
Programadores de sistemas	3%
Consultores	3%
Contadores	2%
Oficiales de seguridad	1%
Contralores	0%
Auditores	0%

Representaciones Gráficas de desastres en computadoras.

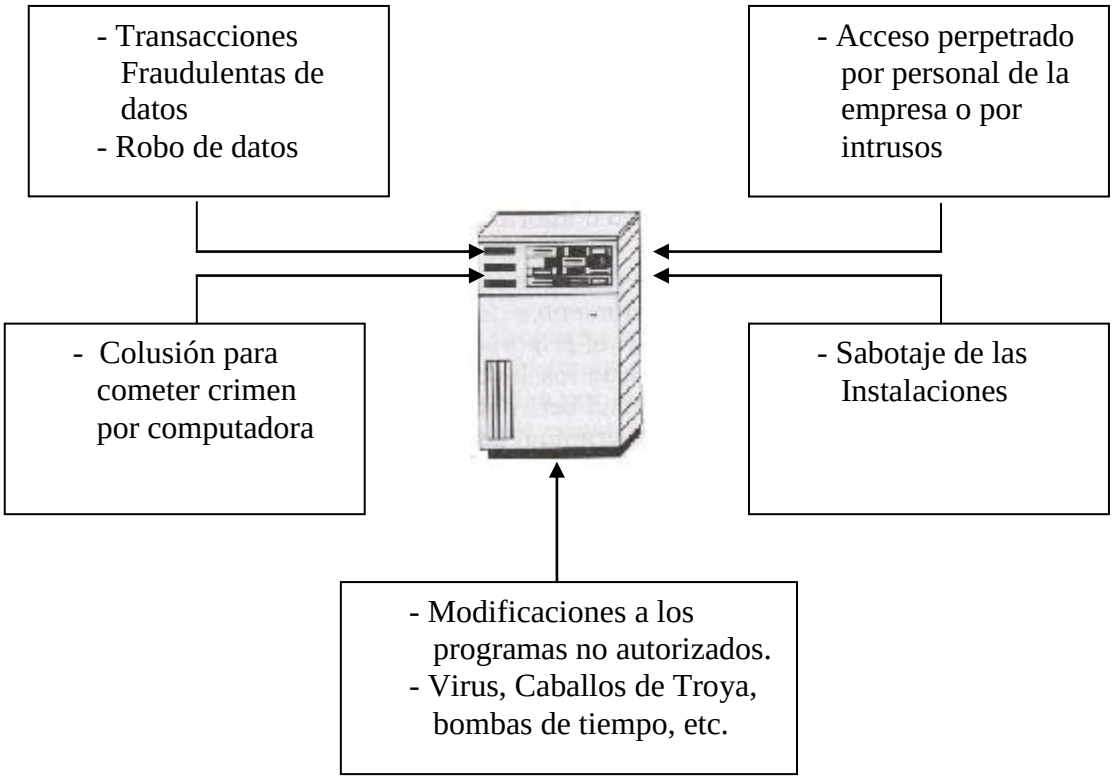


Figura 1.2: Amenazas relacionadas al crimen por computadora.

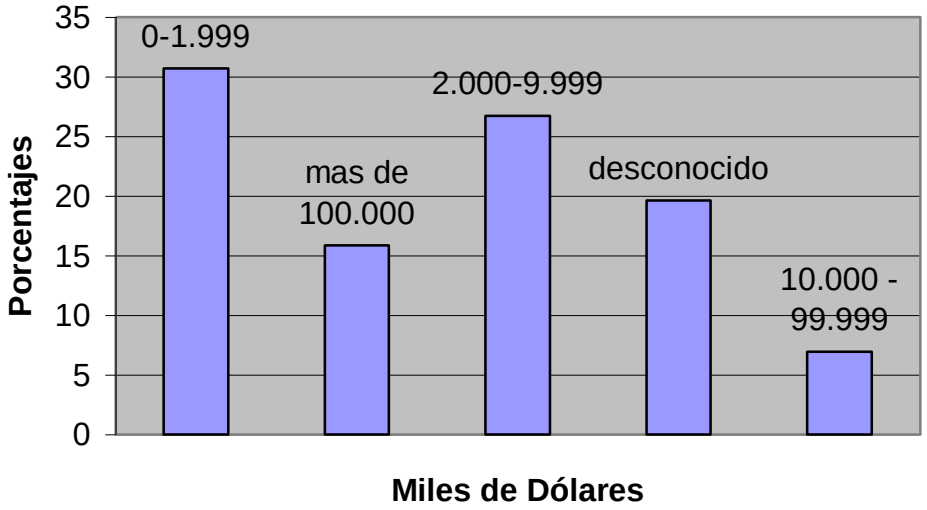


Figura 1.3: Costo de un Desastre Ocasionado por un Virus

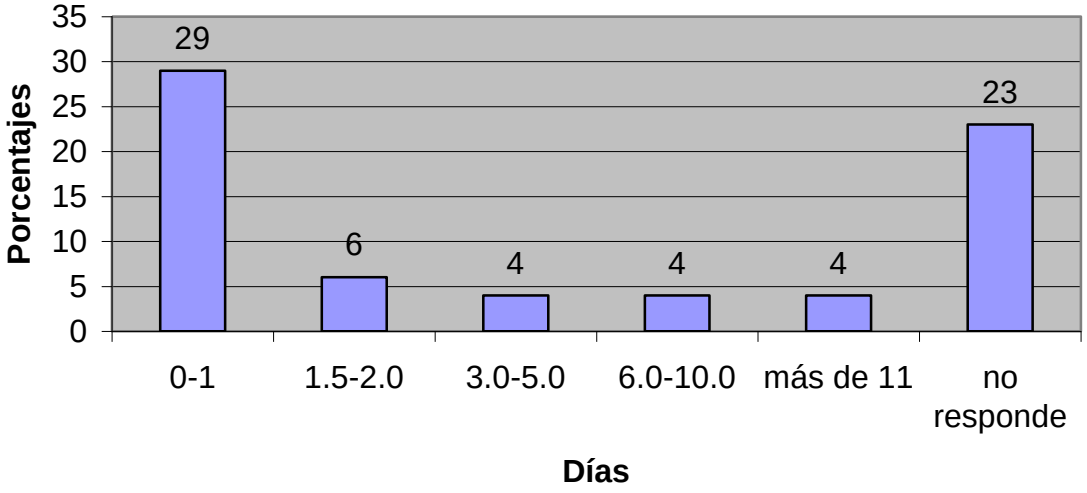


Figura 1.4: Número de Días para una Recuperación Completa después de un Desastre Ocasionado por un Virus

Mencionamos ya que el sabotaje puede tener también el objetivo de destruir físicamente el hardware o los medios de almacenamiento de información, la Figura 1-5 muestra datos al respecto.

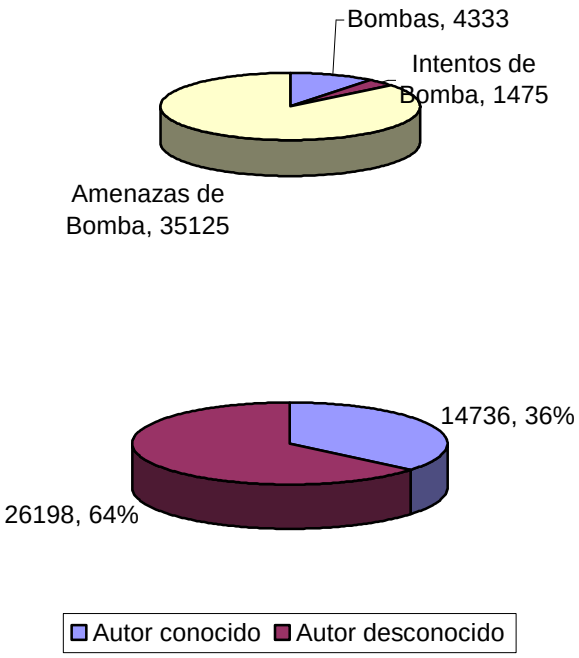


Figura 1.5: Una investigación de bombas y amenazas de bombas en los EE.UU del 1ro de Enero 1969 al 15 de abril 1970

1.6.6. Medidas de prevención y mitigación mediante la clasificación de los Puesto

Se debe clasificar la información según su importancia para la empresa saber qué tanta seguridad se necesita para cada tipo de información, cuánto tiempo necesita ser retenida, a quién se le dará acceso o, se requieren duplicados o no, etc. Es necesario tener bien definido a que información puede tener acceso cada uno de los puestos, Procedimientos de Contratación los procedimientos de contratación incluyen verificar antecedentes penales, referencias y recomendaciones, investigación socio-económica de los aspirantes, entrevista previa, etapa de adoctrinamiento de las políticas de seguridad al empezar a laborar, etc.; *Procedimientos de Terminación del Contrato e*s necesario notificar al área de seguridad cuando un empleado deja de pertenecer a la empresa (de preferencia con anticipación). Se deben recoger sus tarjetas codificadas de acceso, gafetes, equipo propiedad de la empresa, eliminar el acceso a los sistemas de información, tratar de conocer los motivos auténticos de la renuncia, etc.; *Procedimientos de Transferencia* cuando un empleado cambia de puesto

dentro de la empresa deben redefinirse sus accesos a la información (se deben seguir los pasos de un despido y una contratación); *Entrenamiento del Personal d*ebe entrenarse al personal en los procedimientos en caso de emergencia como métodos de evacuación, primeros auxilios, etc. (no olvidemos que el personal es el recurso más importante de las empresas). Se les deben enseñar las políticas de seguridad, los estándares, procedimientos, su responsabilidad individual, etc. Simultáneamente el entrenamiento sirve para ir motivando al personal, para que se interese más por su trabajo, para que valore la lealtad y disciplina en el trabajo, con lo que se reducirá la probabilidad de insatisfacción y el riesgo que esto representa. Como parte de las medidas de seguridad, debe entrenarse a los líderes para que sean capaces de reconocer síntomas de insatisfacción en sus subordinados;

1.6.7. Sistemas de Control de acceso.

Los sistemas de control de acceso permiten tener un registro detallado de los usuarios del sistema, quienes podrán ingresar al sistema de procesamiento de información, además establecer políticas de seguridad a conveniencia del administrador del sistema para el ingreso al mismo, y la vez restringir el ingreso a la información a la que podrían tener acceso los usuarios del sistema.

Hay típicamente tres niveles de controles de acceso que deberían existir cualquier sistema de seguridad de la información:

- Identificación de usuario.
- Password (o contraseña) o número de autentificación de usuario. Se usa para autentificar que la persona es quien dijo al identificarse.
- Mecanismo de autorización. Son los derechos a accesar diversos recursos de un sistema de cómputo y están especificados por reglas de autorización. El mecanismo de autorización es el componente más importante en el sistema de seguridad de la información. Los mecanismos de autorización o paquetes de control de acceso usualmente contienen las siguientes características:
    - identificación de usuario y password.

- salir del sistema si el usuario intenta un password invalido más de un número predeterminado de veces
- controles de autorización que permiten reglas de acceso a los archivos de datos
- reportes de seguridad que resaltan los intentos de acceso no autorizados

La mayoría de los sistemas grandes de cómputo siguen un "principio de default" o un "principio de petición activa". El principio de default consiste en que ningún archivo o conjunto de datos puede ser accesado por un usuario a menos que exista una regla establecida que permita el acceso. El segundo principio significa que se establecen reglas para restringir el acceso: si no hay una regla especifica, no hay restricción de acceso, ¿Cuál es el más conveniente? Depende de la organización del procesamiento de datos, los tipos de información contenidos en los archivos y el compromiso de la organización con la seguridad de su información.

1.6.8. Otros Sistemas

Además de esos sistemas, hay un creciente número de dispositivos de autenticación basados en las características físicas de un individuo, llamados sistemas biométricos, estos son: Sistemas de Voz: Los sistemas de voz son más adecuados para la seguridad física que para seguridad de la información.

- Sistemas de Huella: Desafortunadamente, el margen de error de los sistemas de huellas puede ser alto debido a cortadas, mugre, etc.
- Patrones de Retina: Las tasas de error de los patrones de retina son bajas, pero el costo de estos dispositivos es alto.
- Geometría de la Palma de la Mano: La geometría de la palma de la mano tiene tasas de error bajas y se esta probando en los cajeros automáticos bancarios.

Tiempo de Espera de la Terminal ("Terminal Timeout"): Si después de un cierto tiempo predeterminado no se registra ninguna actividad en la terminal o en la estación de trabajo, debe cerrarse la sesión automáticamente.

Encriptación de Archivos: La encriptación, o codificación de mensajes mediante la criptografía, es el procedimiento más confiable para intercambiar información de manera segura. Básicamente consiste en "disfrazar" o codificar un mensaje mediante algoritmos matemáticos, de forma tal que sólo pueda descifrarlo quien posea la clave de desencriptación.

Figura 1.6: Esquema básico de la encriptación de un mensaje

Restricciones de Tiempo de Acceso: Pueden definirse periodos en los que los usuarios pueden entrar a sus cuentas. Durante el tiempo en que el usuario no tiene necesidad de entrar a su cuenta (fines de semana, por ejemplo) puede denegársele el acceso automáticamente. Cuando el usuario requiere acceso a su cuenta fuera del horario normal de trabajo, deberá requerirlo por escrito al centro de cómputo y al departamento de seguridad de la información.

Detección y Expulsión de Intrusos del Sistema: Debe fijarse un número de intentos de ingresar al sistema. Si se excede este número, automáticamente se bloqueara la cuenta durante un tiempo predeterminado.

Conexiones Concurrentes: No se debe permitir a un mismo usuario tener sesiones simultáneas en diversas terminales, cuando mas procesos se ejecutan concurrentemente pueden presentarse los siguientes problemas:

1. Los procesos pueden estar haciendo uso de datos desactualizados.
2. Los procesos pueden realizar actualizaciones inconsistentes.
3. El sistema puede bloquearse (deadlock).
4. Los datos en diferentes sistemas ejecutándose concurrentemente puede que nunca converjan a un valor consistente o con sentido.
5. Puede ser difícil el problema de sincronización, es decir, el acuerdo entre distintos procesos en relación a una hora común.

Asignaciones de Propiedad (trustee assignments): Desde el punto de vista de seguridad de la información, es muy importante definir bien los privilegios (crear, borrar, modificar, abrir, leer, escribir, etc.) que tiene cada usuario sobre los archivos. Aquí entran nuevamente las consideraciones sobre la "propiedad" de los archivos con el objeto de definir quién puede dar o negar los diversos tipos de acceso a la información y ser responsable de la misma.

Respaldo (Backup): Definir y seguir procedimientos adecuados de respaldo de la información importante de la empresa (tanto de PC como LAN y equipos centrales) representa una actividad de suma importancia en la seguridad de la información y especialmente para la efectividad de los planes de contingencia, deben mantenerse respaldos que contengan los archivos suficientes para recuperar la información dañada o destruida y que garanticen la posibilidad de continuar con el servicio y operación de la empresa, así como los programas y documentación suficiente para facilitar este proceso en sus instalaciones o fuera de ellas.

1.6.9. Ubicación del "Site"

La probabilidad de ser víctima de saboteadores puede minimizarse tratando de situar el centro de cómputo fuera de la vista, y debe ser tan inaccesible como sea posible. La Figura 1-7 muestra un ejemplo de un lugar recomendado para un centro de cómputo, en el que la seguridad es importante. Se necesita protección para las líneas de energía y de comunicación (pueden duplicarse), así como transformadores y otros equipos. Los empleados que no lo requieran, no deben saber dónde se encuentra el almacén de información.

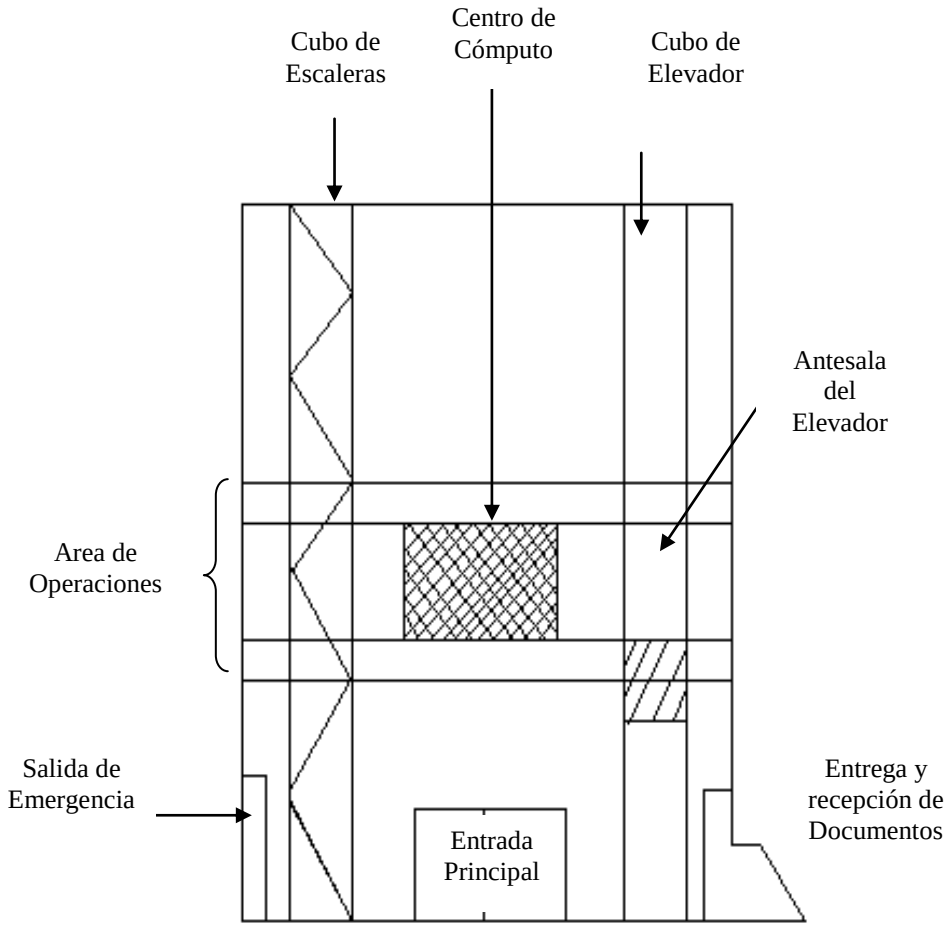


Figura 1.7: Una Ubicación para un Centro de Cómputo en Términos de Seguridad

El Edificio debe tener: Salidas de emergencia controladas. Entradas para recepción y envío controladas.

Control de “paradas” del Elevador.

Area de Operaciones de Procesamiento de Datos.

La persona que lleguen a la antesala del elevador, deben identificarse.

Los pisos inmediatamente arriba y abajo del centro de cómputo deben tener medidas de seguridad reforzada.

Centro de Cómputo: Idealmente debe estar dentro de otro cuarto. Únicamente una entrada. Mínimo número de accesos autorizados. Puerta equipada con dispositivos de control de acceso.

1.6.10. Seguridad del Sistema Operativo

Los sistemas operativos seguros han sido materia de gran preocupación entre los expertos en seguridad de computadoras. Se han hecho esfuerzos considerables para definir y desarrollar lo que se llama un "sistema operativo seguro" (trusted operating system). Los conceptos incorporados en un sistema así están más allá de las necesidades de un sistema de cómputo comercial típico.

El software de control de acceso debe estar diseñado para que las terminales de usuario no puedan obtener acceso directo a las funciones del sistema operativo. Estas funciones incluyen acceso a las librerías de programas y a las diversas tablas del sistema. Debe haber un buen mecanismo para revisar la ocurrencia de cualquier operación inusual.

1.6.11. El Encargado de Seguridad de la Información.

En muchas organizaciones, la seguridad de la información ha sido asignada a individuos como una actividad colateral a sus responsabilidades normales, por lo que recibe poca atención ,la seguridad de la información es demasiado importante para la organización como para ser una actividad eventual.

En la mayoría de las organizaciones, la función de la seguridad de la información debería ser responsable de asignar y controlar passwords, monitorear intentos de acceso impropios, ayudar a revisar aplicaciones nuevas, y promover un conocimiento general de la seguridad de la información dentro de la organización.

El encargado o gerente de seguridad puede ser parte del departamento de procesamiento de datos o, en organizaciones más grande puede estar organizada como una función aparte. En algunas organizaciones, la función de seguridad de la información reporta al encargado de auditoria interna.

1.6.12. Seguridad en Computación del Usuario Final

La protección de la integridad, disponibilidad y confidencialidad de la información para la computación de usuario final requiere gran énfasis en controles básicos de software y medios de almacenamiento similares a los usados en ambiente de computadoras centrales. De cualquier forma deben designarse para ser

administrados en forma descentralizada. La seguridad de la información en sistemas de usuario final puede mantenerse a través de la puesta en práctica de medidas como:

- Respaldo frecuente de información y software, y remoción al almacén off-site, dependiendo de su sensibilidad y valor para la organización.
- Almacenamiento apropiado de disquetes para proteger contra calor o frió extremos, polvo, agua o humedad excesiva.
- Almacenamiento de disquetes en sobres y físicamente alejados de dispositivos magnéticos tales como dispositivos de control de acceso, bocinas, etc.
- Etiquetar apropiadamente y fechar los disquetes para asegurar una identificación positiva de su contenido.

Para mantener el control, la organización debe desarrollar, publicar y hacer cumplir normas de conducta y procedimientos, bajo los cuales cierta actividad personal se considera apropiada o no. La organización estará entonces en posición de monitorear el uso, y cuando se detecte mala conducta, tendrá una base para tomar medidas.

1.7. SEGURIDAD EN REDES Y COMUNICACIONES

1.7.1 Introducción

Dada la importancia fundamental que han adquirido en la sociedad entera (y en especial en las empresas) en nuestros días, las comunicaciones son un recurso que debe protegerse contra cualquier contingencia, Además hay que recordar el alto grado de dependencia que se está dando entre los equipos de cómputo y los equipos de comunicaciones (Ej., computación distribuida), lo que incluso ha dado origen a la Telemática (contracción de Telecomunicaciones e Informática). Por lo tanto es necesario proteger las instalaciones de comunicaciones, ya que a través de ellas se transmite todo tipo de información: voz, datos, etc.

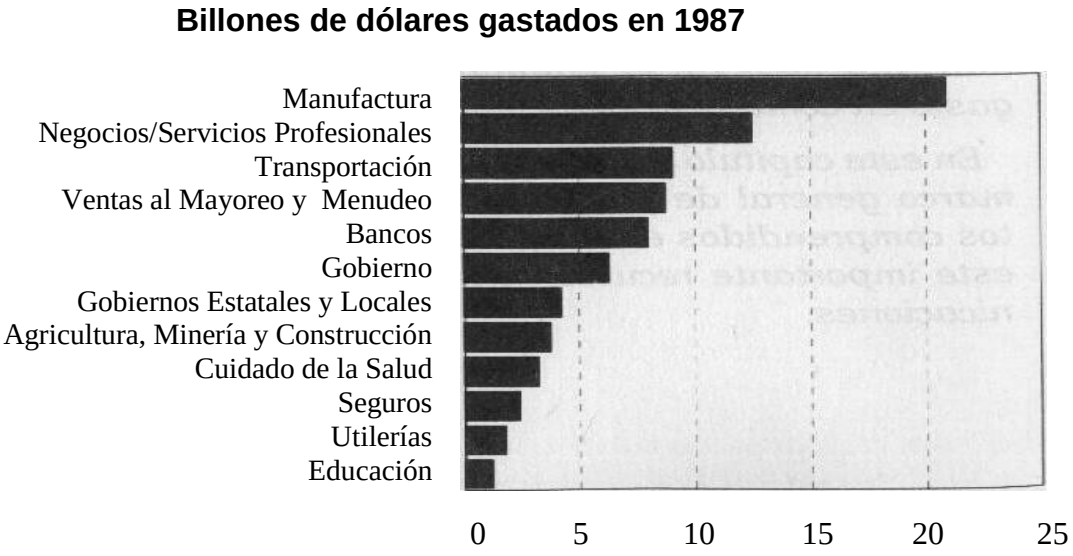


Figura 1.8: Gasto por Industria en Servicios de Transmisión

En los años recientes, el uso de las computadoras ha crecido al punto que hoy está presente en casi cualquier aspecto del mundo de los negocios. Concurrente con este crecimiento ha sido la necesidad de compartir recursos, utilizar mejor equipo, utilizar el trabajo de otros y compartir esfuerzos. La mayoría de los sistemas modernos prácticamente no tendría caso sin la capacidad de comunicarse con otros sistemas. Esta necesidad de compartir y cooperar ha crecido no sólo en términos del número de gente involucrada, sino también en la dispersión geográfica de estas personas y su necesidad de acceso rápido e intercambio de información. Tal crecimiento ha presentado nuevos problemas tecnológicos y operacionales en muchas áreas, particularmente en seguridad de la información. A los dos elementos esenciales de la computación que son el almacenamiento de datos y el manejo de los mismos, ahora se ha agregado la comunicación, con una interrelación cada vez mayor.

1.7.2. Redes de Computadoras

Un grupo de computadoras interconectadas capaces de compartir datos con las otras es llamado red. Las redes de computadoras presentan formidables problemas de seguridad debido a su naturaleza multiusuario, multi-recursos y multi-sistemas.

Así, la vulnerabilidad de la seguridad de una red estriba en que cada nodo no está preparado para un uso compartido por usuarios sobre los que tiene un control limitado o nulo. La seguridad en redes debe ser tan independiente como sea posible de la seguridad de los nodos separados. Sin embargo, los enlaces de datos representan posiblemente el aspecto más vulnerable de cualquier sistema.

En lo que respecta a redes de computadoras, la definición de seguridad implica tres aspectos básicos de protección: (1) proveer acceso controlado a los recursos (identificación y autentificación), (2) Proveer el uso controlado de esos recursos y (3) proveer la seguridad de que el nive1 de protección deseado es alcanzado (monitoreo, etc.).

En este caso, lo que se debe proteger principalmente son las conexiones de tres tipos:

- El enlace tradicional entre una unidad central de procesamiento y terminales remotas. En este grupo se incluyen ahora las conexiones entre microcomputadoras y computadoras centrales.

- La LAN, que permite a las PC compartir recursos a través de líneas de comunicación.

- La red telefónica externa, incluyendo los sistemas de teléfono convencional y otros tipos de servicios públicos de comunicación.

Una razón por la que las redes de comunicaciones han estado tan abiertas a la "invasión" es que muchos usuarios no entienden qué tan vulnerables son.

1.7.3. Consideraciones Especiales para proteger un PC y la Red

Las computadoras personales son un gran problema desde el punto de vista de seguridad, pues bien, las redes de computadoras personales son un problema aún mayor. Las redes de computadoras personales generalmente están entre las instalaciones de cómputo menos seguras. La parte más débil en cuanto a seguridad de una red son las conexiones de comunicaciones, por lo tanto, no sirve de mucho proteger la computadora si la red es vulnerable, esto se aplica a todos los tipos de redes, por lo que la mayoría de las precauciones se deben

aplicar en una LAN. Un problema para la seguridad es que los recursos conectados en red, por definición, están dispersos en varios lugares. Como siempre, se necesita un equilibrio entre la funcionalidad del negocio y la seguridad, aceptando algún riesgo en busca de la eficiencia.

Un sistema completo de seguridad de LAN debería incluir:

- Un sistema de disponibilidad para asegurar que los activos de la red están listos para ser usados por los usuarios autorizados.
- Un sistema de control de acceso que permita que los datos restringidos sean usados únicamente por personas autorizadas.

Un sistema de integridad que protege contra modificación de datos, ya sea accidental o intencionalmente.

1.7.4. Propósito de la Seguridad en Redes y Comunicaciones

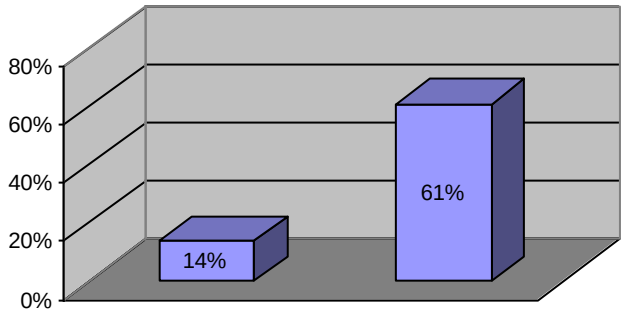
- Preservar la confidencialidad de los datos que pasan a través de cualquier canal de comunicación.
- Asegurar que el mensaje permanezca inalterado durante su transmisión, reteniendo la integridad de los datos que están siendo enviados.
- Asegurar también que realmente estamos conectados con quien creemos que estamos, y ellos (los receptores) deben, a su vez estar seguros de que nosotros somos quienes dijimos que éramos.
- Probar que un mensaje transmitido ha sido recibido exitosamente.
- Asegurar que solamente los usuarios autorizados tengan acceso a la red, controlando el acceso a los componentes de la red y a los passwords.

1.7.5. El Procesamiento Distribuido

El Procesamiento distribuido se entiende como el uso de bases de datos en múltiples máquinas que pueden ser de arquitecturas iguales o diferentes. Como indica la Figura 5-3, la tendencia dentro de las empresas es de confiar cada vez más en una estrategia de procesamiento de datos distribuido.

Empresas usando procesamiento distribuido

Millones de dólares

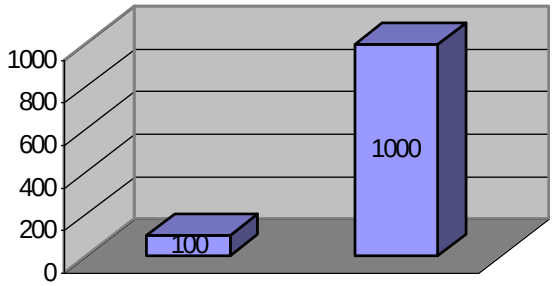


1986 **1990**

Figura 1.9: La Tendencia hacia el Procesamiento Distribuido

Valor del mercado de procesamiento distribuido

Millones de dólares



1986 **1989**

Basado en software y conexiones para todo tipo de comunicación

Figura 1.10: (Cont.) La Tendencia hacia el Procesamiento Distribuido

A continuación se describen algunos de los principales beneficios potenciales y de los inconvenientes potenciales del procesamiento de datos distribuido.

1.7.5.1. Beneficios Potenciales del Procesamiento de Datos Distribuido

Capacidad de Respuesta Las instalaciones de cómputo locales puedan satisfacer más directamente las necesidades de la organización local que las que

están en una instalación central y se pretende que satisfagan las necesidades de la organización completa.

Disponibilidad Con múltiples sistemas interconectados, la pérdida de cualquiera de ellos debería tener un impacto mínimo. Los sistemas y componentes claves se pueden duplicar para que un sistema de respaldo pueda rápidamente tomar el procesamiento después de una falla.

Correspondencia con Patrones Organizacionales Muchas organizaciones emplean una estructura descentralizada con políticas y procedimientos operacionales correspondientes. Los requerimientos por archivos de datos y otros recursos automatizados tienden a reflejar estos patrones organizacionales.

Compartición de Recursos El hardware caro, como las impresoras láser, puede ser compartido entre los usuarios. Los archivos de datos pueden ser manejados y mantenidos centralmente, pero con acceso de toda la organización. Los programas y bases de datos pueden ser desarrollados con base en toda la organización y distribuidos a las instalaciones dispersas.

Crecimiento Gradual En una instalación centralizada, un incremento en la carga de trabajo o la necesidad de un nuevo conjunto de aplicaciones usualmente implica una gran compra de equipo o una actualización o compra importante de software. Esto significa grandes gastos. Con un sistema distribuido, es posible reemplazar gradualmente aplicaciones o sistemas, evitando el "todo o nada". Además se puede dejar que el equipo antiguo corra una sola aplicación si el costo de migrar la aplicación a una nueva máquina no se justifica.

Involucramiento y Control Creciente de los Usuarios Con equipo más pequeño y manejable ubicado cerca del usuario físicamente, el usuario tiene una oportunidad mayor de afectar el diseño y operación del sistema, ya sea por interacción directa con el personal técnico o a través de sus superiores.

Operación Descentralizada y Control Centralizado Las aplicaciones e instalaciones descentralizadas pueden ser diseñada ad-hoc a los requerimientos individuales de las unidades organizacionales y ser mejoradas por servicios y bases de datos centralizadas con van grados de control centralizado.

Productividad del Usuario Final Los sistemas distribuidos tienden a dar mejores tiempos de respuesta al usuario, ya que cada parte del equipo está dedicada a un trabajo más pequeño. También, las aplicaciones e interfaces de la instalación pueden ser optirnizadas a las necesidades de la unidad organizacional. Los gerentes de las unidades están en posición de evaluar la efectividad de la porción local de la instalación y hacer los cambios apropiados.

*Distancia e Independencia de Ubicación L*os sistemas distribuidos que introducen interfaces y métodos de acceso para utilizar servicios de cómputo que se vuelven independientes de la ubicación o distancia. Así, el usuario tiene acceso a instalaciones de toda la organización con poco o ningún entrenamiento adicional.

Prevacía y Seguridad Con un sistema distribuido, es más fácil asignar responsabilidad por la seguridad de los archivos de datos y otros recursos a los propietarios y usuarios de éstos. Se pueden emplear medios físicos y de software para prevenir accesos no autorizados a datos y recursos.

Independencia de Proveedores Puesto en práctica en forma apropiada, un sistema distribuido utilizará software y equipo de una variedad de proveedores. Esto provoca mayor competencia y mejora los precios. La organización es menos propensa a volverse dependiente de un proveedor único y a los riesgos que eso entraña.

Flexibilidad Los usuarios pueden estar en posición de adaptar su software de aplicación a las circunstancias cambiantes sí tienen el control sobre el mantenimiento de programas y las corridas diarias. Debido a que el equipo no es usado por otros usuarios, tienen la capacidad de cambiar configuraciones si lo necesitan.

1.7.5.2. Inconvenientes Potenciales del Procesamiento de Datos Distribuido

Mayor Dificultad para Probar y Diagnosticar Fallas Cuando hay un alto grado de interacción entre elementos de un sistema distribuido, es particularmente difícil determinar la causa de falla o degradación del performance; *Mas Dependencia en Tecnología de Comunicaciones* para que sea efectivo, un sistema distribuido tiene que estar interconectado por instalaciones de redes y comunicaciones. Estas

instalaciones se vuelven críticas para la operación diaria de la organización; *Incompatibilidad entre Equipo e*quipos de diferentes proveedores pueden no conectarse y comunicarse fácilmente. Para garantizar que se evite este problema, el usuario debe restringir aplicaciones y recursos a los que están estandarizados; *Incompatibilidad entre Datos d*e manera similar, los datos generados por una aplicación pueden no ser útiles para otra aplicación. Nuevamente, el usuario puede necesitar restringirse a aplicaciones estandarizadas; *Manejo y Control de Redes* debido a que el equipo está físicamente disperso, a que puede ser de diversos proveedores y a que puede estar controlado por varias unidades organizacionales, es difícil proveer una administración total para forzar el uso de estándares para software y datos, y controlar la información disponible a través de la red. Así, las instalaciones y servicios de procesamiento de datos pueden derivar en algo totalmente fuera de control; Dificultad para Controlar los Recursos Corporativos de Información los datos pueden estar dispersos o, a veces, es el acceso a los datos el que está disperso. Si usuarios distribuidos pueden actualizar la información, se vuelve difícil para una autoridad central controlar la integridad y seguridad de los datos requeridos a nivel corporativo. En algunos casos, incluso puede ser difícil reunir toda la información requerida de las bases de datos dispersas y diferentes; *Suboptimización* con la dispersión de equipo de cómputo y la facilidad de añadir gradualmente equipo y aplicaciones, se vuelve más fácil para los gerentes de suborganizaciones justificar la adquisición de su unidad. Aunque cada adquisición puede ser individualmente justificable, la totalidad de adquisiciones de una organización puede exceder fácilmente el requerimiento total; Duplicación de Esfuerzo el personal técnico puede desarrollar individualmente aplicaciones o archivos de datos similares en varias unidades, ocasionando duplicación de esfuerzo innecesaria y costosa.

1.7.6. Calamidades que afronta una red

Los principales problemas que afronta una red de computadoras al momento de transmitir información de un lugar a otro son:

Intercepción: La intercepción es el robo de información que está siendo transmitida por cualquier medio físico. En el mejor de los casos (pasivo) el intruso

únicamente "escucha" la transmisión, mientras que en el peor (activo), el intruso envía sus propios datos junto con la información legítima o en lugar de ella.

Intercepción Pasiva: Se caracteriza por la intercepción de datos sin su modificación:

- Espionaje. La captura no autorizada de datos transmitidos, ya sea "sacando" la información de la línea, o de las emanaciones emitidas por ésta.
- Análisis de tráfico. Aun cuando el mensaje ha sido encriptado, un análisis de tráfico de la línea puede, en muchas circunstancias, revelar mucho a un extraño.

Intercepción Activa: El atacante realiza acciones para interferir los datos que son transmitidos en un canal de comunicaciones:

- Modificación. El contenido del mensaje puede ser deliberadamente cambiado.
- Re-enrutamiento. El mensaje es desviado a un lugar diferente de su destino.
- Inyección de mensajes falsos.
- Re-envío. El atacante causa que el mensaje tenga que ser repetido varias veces,
- Borrado. El mensaje es borrado.
- Retardo. El mensaje es deliberadamente retardado.
- Disfraz. El atacante finge ser un usuario autorizado.
- Colgarse a la mitad. El atacante se "cuelga" en el enlace entre dos partes que se están comunicando y lleva a cabo dos conversaciones, una con cada parte, convenciéndolos de que están hablando con quien quieren hablar "Entre líneas'. La penetración se hace en el canal de comunicaciones de un usuario legítimo mientras éste no lo está utilizando.

Saturación. Los enlaces ópticos, de radio o microondas pueden ser interferidos con una señal saturadora que "ahoga" la transmisión real.

Ataques Accidéntales: Pueden ser tan dañinos como los ataques deliberados:

- Pérdida de mensaje.
- Duplicación del mensaje.
- Errores de secuencia. El mensaje llega en diferente orden. El texto obviamente se corromperá, pero los errores en números pueden no ser tan obvios,
- Re-enrutamiento de mensajes. El mensaje termina en un destino equivocado.
- Corrupción del mensaje.
- Daño a Infraestructura Externa

El daño a la infraestructura externa es el daño en la infraestructura de la empresa prestadora de servicios portadores (por lo general, la compañía de teléfonos). Desafortunadamente esto es completamente ajeno al usuario de estos servicios.

1.7.7. Consideraciones Especiales (Medidas de Prevención y Mitigación)

Características importantes de la computación distribuida y la de tiempo compartido con respecto a seguridad de la información son las siguientes:

1. La protección se debe basar en métodos de seguridad lógica implementadas en hardware o software, ya que en estos tipos de procesamiento se da poder de cómputo a muchos sitios remotos.
2. Los sistemas deben descansar en métodos de identificación-autentificación, los cuales pueden no ser muy confiables debido a la intervención humana.
3. La seguridad depende mucho de los usuarios de los sistemas "individuales" aceptando y llevando a cabo las prácticas de seguridad.
4. Debido a que los archivos se pueden crear fuera de las estructuras establecidas, el acceso a archivos supuestamente privados puede lograrse

a través de errores de diseño o fallas al crear o aplicar las medidas de protección,

En la computación tradicional, la seguridad lógica es reforzada y complementada por elementos de seguridad física. En la computación distribuida o de tiempo compartido, el usuario puede estar a miles de kilómetros. Por lo tanto la seguridad lógica debe reemplazar la pérdida de control causada por la incapacidad para tener una barrera física de acceso.

Otro punto a considerar son los estándares, los cuales son importantes en todos los aspectos de seguridad, pero especialmente en seguridad de las computadoras. En el contexto de las comunicaciones entre computadoras, quizás más que en cualquier otra parte del mundo del cómputo, esta habilidad de hablar con máquinas que estén en cualquier parte es vital si queremos obtener el máximo beneficio de las inversiones. Con seguridad en redes, es importante que los datos que han sido encriptados en una computadora puedan ser desencriptados en otro sistema autorizado. La American Natíonal Standards Instituto (ANSI) ha emitido varios estándares, que son de los más aceptados.

Manejo de clave: Las claves deben ser generadas, distribuidas, almacenadas, usadas y destruidas sin que sus valores sean divulgados a personas hostiles, e idealmente a ningún ser humano. Los sistemas más seguros s esconden las llaves totalmente, aun de los diseñadores del sistema. El manejo de las claves implica varias técnicas.

- Una llave usada para encriptar otras claves se denominan la maestra y es la más importante.
- La clave de encriptación de datos debe ser cambiada regularmente. cuando menos una vez al día. Por lo tanto, se requiere un mecanismo para enviar las nuevas claves. La forma usual es tener una clave que se usa sólo para encriptar claves de encriptación de datos.
- Periódicamente la clave maestra necesita ser enviada a los receptores en forma muy segura.

- La distribución de claves puede lograrse en varias formas. Supongamos dos partes A y B:
    - La llave podría ser seleccionada por A y físicamente entregada a B.
    - Una tercera parte podría seleccionar la llave y entregarla físicamente a A y a B.
    - Si A y B han usado previa y recientemente una llave, una parte podría transmitir la nueva llave a la otra, encriptada usando la vieja llave.
    - Si A y B por separado tienen una conexión encriptada con una tercera parte C, C podría entregar una llave a través de esas conexiones a A y B.

La opción d) es la más atractiva y podría ser manejada desde una instalación anfitriona o un centro de control de la red. Para este esquema deben identificarse dos llaves:

- Llave de Sesión. Cuando dos sistemas quieren comunicarse, establecen una conexión lógica, durante la cual todos los datos del usuario son encriptados usando esa llave de una sola sesión- Al concluir la sesión, la llave es destruida.
- Llave Permanente. Una llave permanente se usa entre entidades para distribuir llaves de sesión.

Encriptación de Llave Pública: Como vimos, una de las principales dificultades con la encriptación convencional es la necesidad de distribuir las claves en una forma segura. Una buena solución a esto es un esquema de encriptación que no requiera distribución de las claves. Este esquema se conoce como criptografía de clave pública y fue propuesto por primera vez en 1976.

Es posible desarrollar un algoritmo que use una llave para encriptar y otra relacionada pero diferente para desencriptar. Así, funcionará la siguiente técnica:

1. Cada sistema en una red genera un par de llaves para ser usadas en la encriptación y la desencripción de los mensajes que recibirá.
2. Cada sistema publica su llave de encriptación, poniéndola en un archivo o registro público. Ésta es la llave pública. La llave relacionada se mantiene privada.
3. Si A quiere enviar un mensaje a B, encriptar el mensaje usando la llave pública de B.
4. Cuando B recibe el mensaje, lo desencriptar usando la llave privada de B. Nadie más que lo recibe puede desencriptarlo porque sólo B conoce su propia llave privada.

Como se puede ver, la encriptación de llave pública resuelve el problema de la distribución de llaves porque no hay llaves qué distribuir (en forma secreta). Mientras el sistema controle su llave privada, la comunicación que le llegue será segura. Una desventaja importante de esta criptografía con respecto a la convencional es que los algoritmos para encriptación de llave pública son mucho más complejos. Otra desventaja es que, desafortunadamente, un impostor puede generar un par de llaves pública/privada y diseminar la pública como si fuera de otra persona para información más amplia sobre este tema, ver el libro de William Stallings, "Network & Internet work Security", Prentice-Hall, 1995. Una solución es insistir en el intercambio seguro de llaves públicas. Una forma de lograr esto que está siendo ya utilizado por paquetes de seguridad para e-mail, tales como PGR (Pretty Good Privacy) es el "certificado de llave pública".

Autentificación y Firmas Digitales: En el mundo real, la gente hace una gran distinción entre el original y las copias. Un aspecto relacionado con esto, es el de las firmas manuscritas. Para que los sistemas de comunicación entre computadoras sustituyan al transporte físico de documentos, escritos en papel y tinta, debe encontrarse una solución al problema de diseñar un sustituto para las firmas manuscritas. Fundamentalmente, lo que aquí se necesita es un sistema por medio del cual un corresponsal le pueda trasmitir un mensaje "firmado" a otro corresponsal, de tal manera que:

1. El receptor pueda verificar la identidad proclamada por el trasmisor.

2. El transmisor no pueda, posteriormente, negar que envió el mensaje.

Autentificación: En sistemas orientados a conexión, la autentificación puede realizarse en el momento en que se establece una sesión. El planteamiento tradicional consiste en hacer que el usuario compruebe su identidad, mediante la presentación de una contraseña, pero este método expone a1 usuario a una intercepción pasiva, entre otros inconvenientes. Mediante el empleo de la criptografía de llave pública, es posible efectuar la autentificación de una manera confiable.

Aún después de la autentificación inicial, y por razones de seguridad complementaria podría ser deseable que proporcione por lo menos autentificación en cada mensaje. Para esto, puede solicitarse la inclusión en cada mensaje de una contraseña secreta, un número de secuencia, la hora y fecha de transmisión y un código de redundancia, de todos los datos incluyendo el texto en clave completo.

"Firma Digital": Una forma de autentificación es la "firma digital", en la cual el transmisor de un mensaje le pega una identificación codificada, cifrada en tal forma que únicamente el receptor pueda descifrarla y verificar la identidad del transmisor.

Existen firmas digitales con criptografía de llave pública, las cuales pueden aportar una contribución para resolver el problema de que emisores deshonestos repudien sus mensajes anteriores. Una crítica a este método de firma es que junta dos funciones diferentes: autentificación y secreto. En muchas aplicaciones, la autentificación es esencial, pero no así el secreto- Existe un esquema de autentificación que no necesita poner en clave todo el mensaje y está basado en la idea de una función de codificación unidireccional.

Sin embargo, si nos resignamos a tener una autoridad central que lo conozca todo, tanto el secreto como la firma digital pueden obtenerse mediante la criptografía convencional. Una manera de lograr este secreto es exigiéndole a cada usuario que seleccione una clave secreta y se la dé a esa autoridad central. Así, sólo la autoridad y el usuario conocerán su clave secreta.

Enrutamiento Diverso: El enrutamiento diverso consiste en mandar los mensajes separados en Partes y/o por diversos medios.

Call Back Systems: Son sistemas de control de acceso remoto al sistema (a través de MODEM) que funcionan de la siguiente manera; una vez que se ha recibido el número de cuenta y el password y que éstos han resultado correctos, el MODEM cuelga y posteriormente marca al teléfono de donde debe estar terminal que tiene derecho a entrar a esa cuenta.

1.7.8. Protección Física de los Medios de Comunicación

Deben protegerse físicamente las líneas de comunicación y las "cajas" (hubs, mux's, gateways, etc.) en los lugares donde se manda o recibir información ya que es ahí donde se puede interceptar más fácilmente (debido al alto grado de multiplexación utilizado en nuestras comunicaciones. es muy difícil y caro interceptar en otra parte).

1.7.9. Dispositivos de Protección de Puertos

Estos dispositivos de protección de puertos (PPD, por sus siglas en inglés) se ponen físicamente en un circuito para evitar el acceso no autorizado, El PPD se coloca antes de la computadora anfitriona o el MODEM. Estos dispositivos incluyen microprocesadores con lógica programada. Tienen la capacidad de registrar peticiones de entrada y chequear passwords, números de identificación de usuario, u otros códigos, antes de permitir a la terminal el acceso a la computadora anfitriona.

1.7.10. Controles Fundamentales de Seguridad

Con base en estas técnicas de control de acceso y encriptación, se plantean seis controles fundamentales para la seguridad en redes de comunicación.

- Control de integridad: evita la corrupción de los datos por cualquier causa, así como alteraciones, supresiones o inserción de los datos para uso fraudulento.
- Control de autenticidad del origen de tos datos: asegura al destinatario que la información procede del origen que se pretende.

- Control de confirmación: proporciona una prueba al remitente de que el mensaje fue recibido por el destinatario y al destinatario de que el mensaje fue enviado por el remitente.
- Control de confidencialidad: protege los datos contra una revelación no autorizada y asegura que sólo el remitente y destinatario puedan interpretar los datos.
- Control de auditoria: para probar que las transacciones estén libres de error en ciertos eventos selectivos que deben ser registrados y mantenidos en un archivo y poder proporcionar, cuando se requiera, evidencias en caso de fraudes.
- Control de autorización de acceso: evita que terceras personas no autorizadas tengan acceso a información y recursos de cómputo.

1.7.11. Seguridad Técnica para Redes

Independientemente de la técnica específica de seguridad que se decida utilizar, el National Bureau of Standards recomienda que se observen estos cuatro principios:

- Los controles deberían ser parte de un amplio programa de seguridad y manejo de riesgos.
- Cada usuario debería ser identificado en forma única.
- Los controles y el grado de protección deberían corresponder valor de los recursos que se están protegiendo.
- Un dispositivo de control apropiado debería evitar dos clases errores. 1: admitir a alguien no autorizado. 2: negar acceso a alguien autorizado.

. Estos circuitos que responderán a una pregunta enviando el código de identificación del equipo., evidentemente, es necesario proteger esos circuitos de cualquier tipo de intercepción o emanación electromagnética. La calidad de transmisión depende del nivel de ruido del medio y está limitada por el mismo, "Ruido blanco". Identificado por ejemplo por un "hiss" en la línea de audio, y causado por agitación térmica de electrones. "Ruido impulsivo". Una forma de interferencia causada por actividad eléctrica alrededor del medio de

transmisión, originando sonidos repentinos como "elidís" y "Cruce". La interferencia entre líneas adyacentes, en la cual la señal de una se pasa a la otra por inducción electromagnética. En general, cuando las contraseñas u otra información de los usuarios autorizados entran al sistema, es posible que sean interceptados en diversas formas. Para evitar que esto ocurra, es recomendable usar medidas como la encriptación. Idealmente, el proceso de encriptación usado para proteger la información de verificación debe codificarla en forma diferente en cada transmisión, de otra manera, si un enemigo llega a interceptarla, podría utilizarla en ocasiones posteriores sin necesidad de desencriptarla.

1.7.12. Capacidades (Trustee Assígnments)

Cada usuario tiene un conjunto asociado de privilegios de acceso a los cuales está autorizado. A esto se le puede denominar el perfil de capacidades. Por su parte, cada objeto (computadora, área de memoria, archivo, programa, memoria secundaria) tiene asociado un conjunto de requerimientos para su uso, al cual se puede llamar perfil de requerimientos de acceso. Una petición de acceso es autorizada cuando el perfil de capacidades del que lo pide corresponde al perfil de requerimientos de acceso del objeto.

1.7.13. Métodos de Protección Físicos

La segundad física de todos los componentes de un sistema de cómputo, especialmente de aquellas partes que conectan a los diversos elementos es vita1 para e1 esfuerzo general de seguridad. Sin embargo, los enlaces de comunicación a menudo se pasan por alto. Usualmente viajan fuera de1 área de la instalación, saliéndose del ambiente seguro alrededor de la computadora. Considerando su fragilidad, parece sorprendente que los enlaces de comunicaciones sean tan confiables. La protección de los enlaces de comunicación debe concentrarse principalmente en las terminales.

Los enlaces físicos de comunicación siguen rutas predecibles. Se requiere poco esfuerzo para rastrear esas líneas y atacarlas es mucho más sencillo y tiene menor riesgo que atacar el site mismo.

1.7.14. Otros Riesgos y Medidas Preventivas

Existen muchos riesgos de diversas Índoles que afectan a las comunicaciones:

1.7.14.1. Diferencias en la Clasificación

Debe tenerse especial cuidado cuando hay comunicación entre dos sistemas que tienen información de clasificación diferente. Es importante que el sistema menos importante no pueda leer la información clasificada del sistema más alto y que éste no pueda escribir información clasificada al más bajo; a este principio se le conoce como "No Read Up, No write Down". Los reguladores de flujo de datos, que realizan este control forma automática, no están aún ampliamente disponibles.

1.7.14.2. Medidas Diversas de Protección

- El acceso, tanto físico como lógico, a todos los componentes de un sistema de cómputo debe ser estrictamente controlado.
- Cualquier enlace de comunicaciones dentro de un site debería viajar a lo largo de rutas conocidas por las personas autorizadas debajo del piso, dentro de conductos sellados que deben revisarse periódicamente.
- Los cables no deben tener una etiqueta que identifique su función.
- Para reducir las emanaciones y la interferencia (crosstalk) resultante entre cables, debe utilizarse fibra óptica cuando sea posible.
- El tráfico en un enlace de comunicación, especialmente fuera de la organización puede ser rellenado con basura, para esconder la información real y dificultar el análisis de tráfico. Deben utilizarse las rutas más seguras para la transmisión de datos.
- Un enlace de comunicaciones fijo puede ser probado con un dispositivo especial que lee la "firma" del enlace para producir un espectro de señal único. Cualquier interferencia física con el enlace cambiará la "firma".
- De manera similar, los enlaces fijos pueden llevar una señal continua además de cualquier transmisión de datos. Así, cualquier separación del enlace será detectada.

- Emplear sistemas que sólo envían llamadas (out call only systems}. Los sistemas deberían estar diseñados de manera que la computadora central haga todas las llamadas a sitios remotos. Las llamadas que entran no serian reconocidas por el sistema.
- Hay que desconectar las líneas telefónicas de las PC con MODEM cuando éste no sea requerido.
- No debería haber microcomputadoras con MODEM en la red, ya que un MODEM conectado a un nodo de la Lan puede ser punto de acceso para penetrar la red entera.
- Los planes de contingencia deben desarrollarse para contrarrestar cualquier falla "larga" en las comunicaciones.
- Debido a su gran capacidad y a sus características de seguridad (la fibra óptica es casi imposible de interceptar) este medio físico se está usando cada vez más en los edificios de oficinas para transmitir grandes volúmenes de información.

Todas estas medidas específicas contra los peligros que ponen p riesgo la seguridad de las redes y comunicaciones, deben estar en si contexto de toda una estrategia de seguridad que abarque a los otros aspectos de los sistemas de cómputo.

1.8. ENTORNO DE UN PLAN DE CONTINGENCIA

En el mundo de hoy, las organizaciones dependen del procesamiento de datos para el flujo de información esencial. Imagine qué pasaría si se quedara sin procesamiento de datos durante dos días o durante una o dos semanas. Las operaciones comerciales podrían limitarse de tal manera que afectarían los activos corporativos, los movimientos comerciales, el servicio al clientes, el flujo de dinero, las oportunidades de inversión y el margen de competencia, toda organización es vulnerable en caso de que las operaciones de cómputo no funcionen. Las amenazas son reales y un desastre puede resultar de diferentes fuentes, pueden ocurrir desastres naturales, fallas prolongadas de la energía eléctrica, incendios, sabotajes y hasta explosión de bombas. Asimismo, es

importante comprender que un desastre puede ocurrir de la misma manera que producirse. Imagine que se descompone una computadora; inicialmente, esto es sólo un problema, pero si no puede ser reparada en un tiempo razonable, el efecto puede llegar a ser un desastre. Cualquiera que sea la causa, un tiempo prolongado de suspensión del procesamiento de cómputo puede ser devastador, por eso se debe estar preparado. Un plan de recuperación en caso de desastre es una guía para la restauración rápida y organizada de las operaciones de cómputo después de una suspensión. Especifica quién hace qué y cómo. Los objetivos de dicho plan son los de restablecer, lo más pronto posible, el procesamiento de aplicaciones críticas (aquellas necesarias para la recuperación) para posteriormente restaurar totalmente el procesamiento "normal". Un plan de contingencia no duplica un entorno comercial normal (en forma inmediata), pero si minimiza la pérdida potencial de activos y mantiene a la empresa operando, al tomar accione decisivas basadas en la plantación anticipada.

1.8.1 Etapas que constituyen un plan de recuperación

Dentro de lo que se denomina un plan de recuperación existen etapas, a la vez cada etapa se encuentra constituida por actividades que deben cumplirse para conseguir el objetivo que persigue cada una de las etapas, un plan de recuperación se encuentra constituido por cuatro etapas, siendo estas: Planificación, Análisis de Riesgos, Gestión de riesgos, y Selección de Salvaguardas.

1.8.1.1. Etapa 1: Planificación del Análisis y Gestión de Riesgos

Objetivo: Es establecer y definir el marco general de referencia para todo proyecto de realización de análisis y gestión de riesgos. Existen objetivos complementarios que coayudan en cumplir el objetivo principal siendo estos objetivos complementarios:

- Motivar a la Dirección de la Unidad implicada,
- Demostrar la oportunidad de realizar un Análisis y Gestión de Riesgos,
- Afirmar y dar a conocer la voluntad política de la realización por parte de la Dirección, Crear las condiciones para el buen desarrollo del proyecto.

El contenido de esta etapa se enmarca, en como ocurre con cualquier otra planificación concreta, en la Planificación estratégica de la Organización tiene como finalidad principal definir las metas de ésta a largo plazo (en cuanto a funcionalidades y servicios futuros a prestar, perspectivas de crecimiento y/o previsiones de evolución), así como estimar las necesidades de información en función de dichas metas (considerando tanto la situación de la Organización frente a su entorno, como la visión de los responsables de la misma). Esta etapa de planificación concreta la realización "táctica" de las metas estratégicas definidas en la planificación estratégica, con dos grandes resultados:

- La definición precisa del proyecto de Análisis de Riesgos y de su dominio.
- La Programación ajustada para desarrollar el proyecto, teniendo en cuenta las prioridades y los recursos necesarios, es decir:
    - La definición de la serie de hitos a considerar en el desarrollo del proyecto
    - La obtención de unos resultados que sirvan de punto de partida al desarrollo del proyecto.

Como consecuencia lógica, esta etapa de planificación requiere:

- Un ámbito organizativo más restringido y un horizonte temporal más limitado
- Un trabajo sucesivo de refinamiento y revisión a lo largo del desarrollo del proyecto de manera que se pueda valorar el cumplimiento de su programación en el marco de metas establecidas por la Planificación Estratégica
- La participación imprescindible de los responsables de las Unidades implicadas, puesto que les corresponde definir los objetivos y las estrategias de evolución de dichas unidades, así como patrocinar todos los trabajos encaminados a obtener la seguridad de sus sistemas como uno de los retos básicos de un entorno en constante evolución.

En resumen, el contenido de esta etapa como marco general de referencia incluye:

- La justificación y oportunidad de abordar el proyecto.
- La definición del dominio a considerar y de los objetivos del proyecto.
- La planificación del proyecto, considerando los participantes, los recursos necesarios y el cronograma de realización
- La particularización de las técnicas a emplear en las actividades del proyecto.

Actividad 1: Oportunidad de realización

Se estudian los aspectos básicos para la realización de un proyecto de análisis y gestión de riesgos, fundamentando la oportunidad de ésta. Se inicia una primera aproximación a los objetivos asignados al proyecto, al dominio o ámbito a incluir y a los medios necesarios para su elaboración. Esta actividad tiene como objetivo suscitar el interés de la Dirección de la Organización en la realización de un proyecto de análisis y gestión de riesgos, la dirección de la organización suele ser consciente de las ventajas que aportan las técnicas electrónicas, informáticas y telemáticas a su funcionamiento, pero no de los nuevos problemas de seguridad que estas técnicas implican.

Tarea 1: Clarificar la oportunidad de realización.- La iniciativa para la realización de un proyecto de análisis y gestión de riesgos parte de un promotor interno o externo a la organización, consciente de los problemas relacionados con la seguridad de los sistemas de información, como por ejemplo:

- Incidentes continuados relacionados con la seguridad.
- Inexistencia de previsiones en cuestiones relacionadas con la evaluación de necesidades y medios para alcanzar un nivel aceptable de seguridad de los sistemas de información que sea compatible con el cumplimiento correcto de la misión y funciones de la Organización.
- Reestructuraciones en los productos o servicios proporcionados.
- Cambios en la tecnología utilizada.
- Desarrollo de nuevos sistemas de información.

El promotor puede elaborar a partir de lo anterior un cuestionario para promover la reflexión sobre aspectos de la seguridad de los sistemas de información por parte de:

- **Los responsables de las Unidades.** El cuestionario permite proceder a un examen superficial de la situación en cuanto a la seguridad de sus sistemas de información; deben poder expresar su opinión por los proyectos de seguridad ya realizados (con su grado de satisfacción o con las limitaciones de éstos), así como sus expectativas ante la elaboración de un proyecto de análisis y gestión de riesgos. Esta aproximación de alto nivel permite obtener una primera visión de los objetivos concretos y las opciones políticas que tendrían que subyacer a la elaboración del proyecto de análisis y gestión de riesgos.
- **Los responsables de informática.** El cuestionario permite obtener una panorámica técnica para la elaboración del proyecto de análisis y gestión de riesgos y posibilita abordar el estudio de oportunidad de realización del proyecto, tras integrar las opciones políticas anteriores.

Con estos elementos el promotor realiza el informe preliminar recomendando la elaboración del proyecto de análisis y gestión de riesgos e incluyendo estos elementos:

- Exposición de los argumentos básicos.
- Especificación de los antecedentes sobre seguridad de sistemas de información (por ejemplo un plan estratégico de la propia organización, un Plan de actuación del ministerio, Departamento, Unidad, etc.).
- Primera aproximación del dominio a incluir en el proyecto en función de
    - Las finalidades de las unidades.
    - Las orientaciones políticas y técnicas retenidas.
    - La estructura organizativa.
    - El entorno técnico.

- Primera aproximación de los medios, tanto humanos como materiales, para la realización del proyecto de análisis y gestión de Riesgos (AGR)-

El promotor presenta este informe preliminar a la Dirección que puede decidir:

- Aprobar el proyecto, o bien
- Modificar su dominio y/o sus objetivos, o bien
- Retrasar el proyecto.

Actividad 2: Definición de dominio y objetivos

Se definen los objetivos finales del proyecto, su dominio y sus límites. Se realiza una primera identificación del entorno y de las restricciones generales a considerar. Se establecen los colectivos (responsables, técnicos , usuarios, etc) a considerar para la recogida de información. Una vez que se ha constatado la oportunidad de realizar el proyecto de Análisis y Gestión de Riesgos y el apoyo por la dirección, esta actividad procede a identificar los objetivos que debe cumplir el proyecto y a definir su dominio y límites.

Tarea 1: Especificar los objetivos del proyecto.- Permite determinar el alcance del proyecto y de sus objetivos, diferenciados según horizontes temporales a corto y mediano plazo. Los objetivos del proyecto se especifican en función de la finalidad de la planificación estratégica, del estado de partida de la organización y de las consideraciones de la Dirección recogidas en la actividad anterior. Esta especificación de objetivos determinaría por ejemplo que el proyecto busca determinar las áreas de riesgo más elevado en la organización (Objetivo Reducido).

Tarea 2: Definir el dominio y los límites del proyecto.- Identificar las Unidades objeto del análisis y Gestión de Riesgos y especifica las características generales de dichas unidades en cuanto a responsables, servicios proporcionados o ubicaciones geográficas. También identifica las principales relaciones de las Unidades objeto del proyecto con otras entidades por ejemplo el intercambio de información en diversos soportes, el acceso a medios informáticos comunes, etc. La tarea parte de un principio básico: el análisis y la gestión de riesgos debe

centrarse en un Dominio limitado, que puede incluir varias unidades o mantenerse dentro de una sola unidad orgánica (según la complejidad y el tipo de problema a tratar), ya que un proyecto de ámbito demasiado amplio o indeterminado podría ser inabarcable, por excesivamente general o por demasiado extendido en el tiempo, con perjuicio en las estimaciones de los elementos del Análisis y Gestión de Riesgos.

Tarea 3: Identificar el entorno y las restricciones generales.- Realizar un estudio global de los sistemas de información de las Unidades incluidas en el dominio del proyecto, con objeto de identificar sus funciones y finalidades principales y sus relaciones con el entorno, así como sus tendencias de evolución. El perfil general de las Unidades, producto obtenido en la tarea anterior, se amplia en ésta con la información proporcionada por los responsables de las diversas áreas de dichas Unidades.

La tarea también identifica las personas a entrevistar para obtener la información que posibilite la Etapa 2 de análisis de riesgos y las posibles restricciones generales que deberá tener en cuenta el proyecto. Para incorporar las restricciones al análisis y Gestión de Riesgos, se agrupan por distintos conceptos. En esta tarea se adopta la siguiente clasificación de restricciones en 6 grupos: temporales, financieras, técnicas, sociológicas, del entorno, legales.

Actividad 3: Planificación del Proyecto

Estimar los elementos de planificación del proyecto, es decir sus cargas de trabajo, el grupo de usuarios, los participantes y su modo de actuación y el plan de trabajo para la realización del proyecto. En dicha estimación se ha de tener en cuenta la posible existencia de otros planes (por ejemplo un Plan Estratégico de Sistemas de Información o de Seguridad general de las Unidades que pueden ser afectadas o en la Organización) y el plazo de tiempo considerado para la puesta en práctica del proyecto de Análisis y Gestión de Riesgos.

Tarea 1: Evaluar cargas y planificar entrevistas.- Para evaluar el tiempo y los efectivos necesarios en la realización del análisis y gestión de Riesgos, la tarea establece los parámetros a estudiar en función de las finalidades de las unidades y de los ámbitos de su actividad, fijando en función de la “malla” de estudio

elegida el grado de detalle al que conviene llegar en la cuantificación de dichos parámetros. La tarea por lo tanto permite:

- Identificar, por ámbitos y temas, a los usuarios afectados.
- Planificar la composición, papel y contribuciones respectivas de los grupos de usuarios
- Evaluar la carga de trabajo y deducir la composición del equipo de proyecto a constituir, en términos de competencia técnica y de efectivos.
- Planificar las entrevistas a realizar con los usuarios para la recogida de información.

Tarea 2: Organizar a los participantes

Esta tarea permite:

- Determinar los órganos participantes en la gestión, realización, seguimiento y actualización del proyecto de análisis y gestión de riesgos.
- Definir las funciones y responsabilidades de los órganos participantes.
- Establecer las reglas y los modos operativos.

Los participantes en un proyecto de análisis y gestión de riesgos se articulan en estos órganos.

- **Comité de Dirección:** Está constituido por los responsables de las unidades afectables por el proyecto de análisis y gestión de riesgos, así como por los responsables de la informática y de la gestión dentro de dichas unidades. También será importante la participación de los servicios comunes de la Organización (programación y presupuesto, Recursos Humanos, Administración, etc).
- **Director del Proyecto:** Debe ser un directivo de alto nivel, responsable dentro de la Organización de Seguridad, de Sistemas de Información o, en su defecto, de Planificación, de Coordinación o de materias, servicios o áreas semejantes.

- **Equipo de Proyecto:** Formado por personal experto en Tecnologías y Sistemas de Información y personal técnico cualificado del dominio afectado, con conocimiento de gestión de seguridad en general y de la aplicación de la metodología de análisis y gestión de riesgos en particular. Si el proyecto se hace con asistencia técnica mediante contratación externa, el subsiguiente personal especialista en seguridad de sistemas de información se integrará en este equipo de proyecto.
- **Enlace operacional:** Será formado por usuarios representativos dentro de las unidades afectadas por el proyecto de análisis y gestión de riesgos. Lo constituyen varios posibles subgrupos:
    - Informáticos (analistas, diseñadores, programadores, gestores,...).
    - Usuarios (gestores, finales,...).
    - Otros (seguridad física, calidad, mantenimiento, compras,...).

La constitución de un grupo de calidad diferenciado del grupo de Usuarios y la amplitud relativa de los diversos grupos de participantes dependerá de los objetivos y envergadura del proyecto, así como del dominio considerado.

Tarea 3: Planificar el trabajo.- Para esta tarea se realiza las funciones siguientes:

- Elaborar el calendario concreto de realización de las distintas etapas, actividades y tareas del proyecto especificado de análisis y gestión de riesgos, en función de sus objetivos y características definidas previamente.
- Especificar los recursos humanos y materiales estimados para el cumplimiento y desarrollo de cada etapa.
- Establecer un calendario de seguimiento que define las fechas tentativas de reuniones del comité de Dirección, el plan de entregas de los productos del proyecto, las posibles modificaciones en los objetivos marcados, etc.

Actividad 4: Lanzamiento del Proyecto

Esta actividad completa las tareas preparatorias del lanzamiento del proyecto de análisis y gestión de riesgos: empezando por seleccionar los criterios y las técnicas concretas a emplear en el análisis y gestión de riesgos; y terminando por asignar los recursos necesarios para la realización del proyecto y por realizar la campaña informativa de sensibilización a los implicados en el proyecto.

Tarea 1: Adaptar los cuestionarios.- La tarea adapta los cuestionarios a utilizar en la recogida de información de la siguiente etapa, en función de los objetivos del proyecto, del dominio y de los temas a profundizar con los usuarios, identifican correctamente los elementos y otros condicionamientos principales del análisis y gestión de riesgos (activos, amenazas, vulnerabilidades, impactos, salvaguardas existentes, restricciones,..).

Tarea 2: Seleccionar criterios de evaluación y técnicas para el proyecto.- Esta tarea, preparatoria de la Etapa 2 de análisis de Riesgos, establece la selección cuando cabe del os criterios y técnicas que se mantendrá a lo largo de todo el proceso de análisis y gestión de riesgos. En efecto, la gestión de los riesgos de la etapa 3 estará condicionada por el tipo de análisis de riesgos realizado en la etapa 2. Si se han elegido un tipo de criterios y técnicas para evaluar los riesgos, es recomendable aplicar las mismas técnicas para evaluar la reducción de riesgos al implantar las salvaguardas propuestas. La elección de estos criterios y técnicas en función de:

- Los objetivos del proyecto
- El dominio del proyecto
- El tipo de proyecto

Tarea 3: Asignar los recursos necesarios.- Asignar los recursos necesarios (humanos, organizacionales, técnicos, etc.) para la realización del proyecto de análisis y gestión de riesgos.

Tarea 4: Sensibilizar (Campaña informativa).- Informar a las unidades afectadas del lanzamiento del proyecto de análisis y gestión de riesgos, por diversos medios, y como mínimo:

- Una nota informativa de la dirección, dirigida a las unidades implicadas y declarando su apoyo a la realización del proyecto.
- La presentación del proyecto, sus objetivos y la metodología a emplear, realizada en las unidades implicadas por parte del equipo de trabajo.

1.8.1.2. Etapa 2: Análisis de Riesgos

Objetivos de la etapa:

- Evaluar el riesgo del sistema en estudio, tanto el riesgo intrínseco (sin salvaguardas), como el riesgo efectivo (incluyendo el efecto de las salvaguardas implementadas si se trata de un sistema actual, no de un sistema previsto).
- Mostrar al comité director las áreas del sistema con mayor riesgo.
- Presentar y obtener la aprobación de los umbrales de riesgo aceptables o asumibles.

El punto de partida de esta etapa empieza con la culminación de la etapa anterior y documentación obtenida de la misma, referente a los objetivos del proyecto, los planes de entrevistas, la evaluación de cargas, la composición y reglas de actuación del equipo de participantes, el plan de trabajo y el informe de presentación del proyecto. El análisis del riesgo identifica los elementos definidos en el correspondiente submodelo, con el resultado de una evaluación del riesgo en el dominio del proyecto que sea utilizable para la identificación y gestión de las salvaguardas que puedan contrarrestar el riesgo no asumible. La etapa de análisis de riesgos sigue en cierta forma el subescenario de ataque de la vista dinámica “organizativa” del submodelo de Eventos, combinando en cada uno de los “pasos” del subescenario operaciones relacionadas con los elementos de seguridad. Así y tras definir más detalladamente el contenido del dominio (es decir el conjunto de activos), la etapa considera los posibles eventos (o se las

amenazas), la potencialidad de la materialización de éstas y las consecuencias de dicha materialización (los Impactos).

Con ayuda de todos estos materiales, suficientemente identificados y evaluados, el cálculo o la estimación de los distintos tipos de riesgos es una labor bastante rutinaria.

Recolectar la información sobre el sistema y de los factores que pueden influir en la seguridad. Esta actividad tiene una importancia crucial por dos motivos: la información a recoger condiciona el conocimiento del equipo del proyecto (ajeno en parte al funcionamiento del Dominio o sea dependiente de los conocedores de su comportamiento cotidiano); y la recogida en sí es una operación delicada que exige una confianza mutua profunda (la transmisión de información es siempre delicada y más si concierne a la seguridad).

Tarea 1: Preparar la información.- Esta tarea comprende las siguientes Acciones encaminadas a preparar la recogida de la información:

- Recopilar los cuestionarios personalizados distribuidos en la etapa anterior.
- Ubicar y localizar a los entrevistados, para optimizar la realización de las entrevistas, tanto espacial como temporalmente.
- Confirmar cada entrevista, informando de los documentos que se van a requerir durante la entrevista, para facilitar su disponibilidad
- Recordar los objetivos de cada entrevista al entrevistado.
- Disponer del documento acreditativo de la Dirección.

Tarea 2: Realizar las entrevistas.- Profundizar con los entrevistados los siguientes aspectos:

- Definición de las funciones y objetivos del entrevistado.
- Descripción del modo de actuación.
- Identificación de los medios de que dispone para realizar las funciones y del personal a su cargo.
- Identificación de los procesos realizados y de la información manejada.

- Descripción del entorno.
- Identificación de posibles situaciones conflictivas (internas o externas, accidentales o provocadas).

Durante la entrevista, suele ser necesario informar al entrevistado de los principales conceptos relacionados con la seguridad y la de los sistemas de información, en un grado que depende de su información y experiencia en la materia. Con estos preparativos, la entrevista permite realizar una primera adquisición de conceptos y datos sobre elementos de la seguridad como los siguientes:

- Delimitación de los activos.
- Valor de reposición de los activos, si tiene sentido o es factible.
- Importancia de los activos para el sistema organizacional del entrevistado.
- Salvaguardas existentes.
- Amenazas potenciales.
- Incidentes, y en el caso de que hayan ocurrido, las consecuencias derivadas de éstos (pérdidas materiales, inmateriales, etc.).
- Planos y distribución geográfica pertinentes en materia de riesgos.

Asimismo, la entrevista permite apreciar otros extremos:

- Umbral de riesgo y aspectos de la seguridad en los que será necesario concentrarse.
- Restricciones a tener en cuenta (económicas, temporales, etc.).
- Aspectos organizativos.
- Especificación de normas y estándares.
- Procedimientos de explotación.

Tarea 3: Analizar la información recogida.- Permite realizar una síntesis de la información obtenida en las entrevistas realizadas, que se refleja en las correspondientes actas de reunión. Éstas permiten, una vez redistribuidas a los entrevistados, confirmar y depurar los datos recogidos. Las actas de reunión se

actualizan con las modificaciones propuestas para obtener las actas definitivas. La información obtenida en las entrevistas se completa en los casos necesarios con:

- Si se han realizado inspecciones operacionales, las observaciones del auditor o del analista experto en seguridad.
- Las observaciones de expertos en temas relacionados con la Seguridad de los Sistemas de Información, de forma que se detecten los puntos no evidentes, los activos encubiertos, las frecuencias de las amenazas generadas por nuevas tecnologías.
- La recopilación de información de otras fuentes, como por ejemplo, estudios estadísticos sobre ocurrencia de desastres naturales (que puedan afectar al sistema), estadísticas de fallos en los componentes (MTBF o de Tiempo Medio entre Fallos, que posiblemente se encuentran en los manuales de características técnicas del componente), número de errores por millón de instrucciones en los programas, etc.

Se elabora un informe recopilador con todos los aspectos de la información recogida de las distintas Unidades y con las consideraciones que el analista de seguridad puede incorporar. Se incluirán como anexo las actas de reunión de las entrevistas realizadas.

Actividad 2: Identificación y agrupación de ACTIVOS

En la etapa de definición del dominio se han descrito las funciones que se realizan, ponderadas además según su importancia para la misión de la organización. El objetivo de esta actividad es reconocer los activos que componen los procesos, y definir las dependencias entre ambos. Así y a partir de la información recopilada en la actividad anterior, esta actividad profundiza el estudio de las activos con vistas a obtener la información necesaria para realizar las estimaciones del riesgo.

Tarea 1: Identificar activos y grupos de activos.- Para gran parte de Activos materiales y algunos inmateriales (los llamados a ser un inventario), la tarea puede arrancar de los correspondientes Inventarios valorados que se desarrollan

para otros fines (por de pronto para la valoración anual del Patrimonio de la Organización que forma parte obligatoria de toda Contabilidad General por partida doble). Esta valoración 'oficial' de muchos Activos ayuda también fundamentalmente a arrancar la Tarea siguiente, que se centrará en valorar los Activos identificados por la tarea actualmente descrita.

La tarea clasifica los Activos identificados en las tipologías ofrecidas y los agrupa según una consideración principal de jerarquía organizativa y según otras posibles consideraciones:

- Subestados de seguridad (Autenticación, Confidencialidad, Integridad, Disponibilidad, referenciados brevemente como A-C-I-D).
- Amenazas que los pueden atacar,
- Salvaguardas que los pueden proteger.

La tarea se completa añadiendo en el registro de cada Activo otros campos pertinentes para su tratamiento posterior: descripción, ubicación, responsable encargado, número o cantidad, etc. La tarea agrupa Activos articulándolos en conjuntos definidos por el objetivo común de realizar un tipo de función determinada (que a su vez es un componente de la misión del sistema). La agrupación de Activos más práctica desde el punto de vista del Análisis de Riesgos los articula en los 5 niveles de capas considerados.

1. entorno
2. sistema de información
3. información
4. funcionalidades de la Organización
5. otros activos

Una cadena 'vertical' concreta o 'árbol de Activos' tomados de estas capas agrupa los Activos afectables por el desencadenamiento potencial de una Amenaza determinada. Por ejemplo, la amenaza de un ladrón aprovecha la vulnerabilidad de una puerta abierta en el despacho del director financiero por el personal de limpieza fuera del horario de trabajo para robar un PC (entorno, capa

1) con sus programas (sistema de información, capa 2), lo que desencadena una carencia (de información, capa 3) crítica para el mantenimiento de la Organización (funcionalidades, capa 4). Aunque la información se pueda recomponer (preguntando a los bancos con los que la Organización opera) es inevitable la mala imagen causada y es posible el falseamiento de datos, sin mencionar el mal uso por revelación que puede resultar del robo del contenido, si ha sido intencionado (otros activos, capa 5).

Adicionalmente y por otro lado, la Tarea puede preparar potestativamente otro tipo de agrupación basada en la naturaleza de los Activos, para facilitar el estudio de los mecanismos de salvaguarda ya implantados o a implantar en aquellos. Por ejemplo, un computador personal PC, formado por varios activos como monitor, teclado, CPU, periféricos, sistema operativo, aplicaciones, datos, etc. puede ser atacado en su conjunto por determinadas amenazas y requiere mecanismos de salvaguarda adaptados individualmente a cada activo y colectivamente al PC conjunto. Este tipo de agrupación de Activos recoge grandes áreas tradicionales como éstas:

- Información y datos.
- Hardware.
- Software operativo.
- Software de aplicación.
- Comunicaciones.
- Documentos.
- Equipamiento ambiental.
- Personal interno y externo.
- Infraestructura.
- Activos organizacionales.

Tarea 2: Identificar los mecanismos de salvaguarda existentes.- Paralelamente a la Tarea anterior de identificación de los activos, esta Tarea permite identificar los mecanismos de salvaguarda asociados o implantados en

aquellos, describiéndolos y descubriendo la contribución de los mismos a los distintos subestados de seguridad de los Activos (Autenticación, Confidencialidad, Integridad, Disponibilidad, A-C-I-D). Además, la Tarea obtiene información de los costes de la implantación y de mantenimiento anual de dichos mecanismos.

Tarea 3: Valorar activos.- La tarea arranca de los ***Inventarios*** valorados ya utilizados en la tarea anterior y permite dos valoraciones de los Activos, una intrínseca y otra asociada a sus subestados de seguridad (autenticación, confidencialidad, integridad, disponibilidad).

- **Valoración intrínseca.** Los activos inventariables permiten la asociación de un valor monetario derivable, a efectos de cuantificar posibles Impactos, del valor patrimonial 'oficial' reseñado en el inventario (valor de reposición, valor de cambio, coste de producción en horas/hombre por precio/hora, etc.). Los activos no inventariables no permiten dicha asociación directa de un valor monetario, pero esto no impide que en la mayor parte de los casos se pueda ponderar su valor de uso, por ejemplo considerando las consecuencias económicas que supondría su carencia. El procedimiento recomendado para valorar activos se puede resumir en un doble esfuerzo:

    a. Debe intentarse encontrar el 'valor de cambio' del activo como valor de reposición, directa (valor de inventario) o indirectamente (coste de su regeneración tras un Impacto)

    b. Si esa valoración fuera imposible o inconveniente (valor de 'reposición' de una persona tras un accidente causado por falta de seguridad de algún activo), debe de tratarse este activo (con sus posibles impactos y riesgo consecuentes) como un elemento del entorno del Dominio abarcado por el proyecto de seguridad

- **Valoración asociada a los subestados de seguridad.** Proporciona un valor cualitativo de los subestados de seguridad del Activo (autenticación, confidencialidad, integridad, disponibilidad, A-C-I-D), tomando como referencia el grado de cumplimiento de la función y la importancia del activo para la misión del sistema. Este tipo de 'valoración asociada a los

subestados de seguridad' también permitirá en el estudio de valoración del impacto una primera aproximación alternativa a la 'valoración intrínseca'.

La Tarea también genera los niveles globales para todo el Dominio de los subestados A-C-I-D de seguridad a partir de los niveles de los subestados A-C-I-D de cada elemento y con ayuda de las agrupaciones indicadas en la Tarea anterior.

Actividad 3: Identificación y evaluación de AMENAZAS.- La Actividad permite identificar y evaluar las amenazas que sufren los activos del sistema. Cada Amenaza es un evento que potencialmente puede desencadenar otras amenazas. Todas juntas constituyen un 'escenario de amenazas', que desencadena un "árbol de fallos" como subescenario de ataque real a un "árbol de activos" (determinado en la Actividad anterior). La Vulnerabilidad asociada al "árbol de Activos" y específica para el "escenario de amenazas", propicia el desencadenamiento de éstas que producen Impactos (es decir deterioros) en los Activos afectados, con distintos grados posibles de profundidad. La actividad simplifica el subescenario de ataque complejo y recursivo de los "árboles de fallos" afectando a "árboles de activos" y lo divide en dos análisis semiautónomos realizados en las dos tareas sucesivas siguientes.

Tarea 1: Identificar y agrupar amenazas.- Identifica las amenazas y establece su tipología así como sus orígenes y sus objetivos principales o secundarios.

- La tipología atiende a la "naturaleza" de las amenazas (clasificables como accidentes, errores, intencionales presénciales e intencionales teleactuadas).
- Entre los orígenes puede que interese identificar los agentes de las amenazas y ciertas características como su capacidad de y oportunidad de acción, así como su motivación en el caso de amenazas intencionadas.
- Los objetivos de las amenazas son los 'árboles de activos' que aquéllas pueden afectar.

Tarea 2: Establecer los árboles de fallos generados por amenazas.- Establece las dependencias entre amenazas identificadas en la tarea anterior, sin

tener en consideración por el momento los “árboles de activos” afectados, de forma que se articulen agrupaciones de amenazas cuyo denominador común es su desencadenamiento y actuación conjunta, en el caso de materialización de alguna de ellas.

Actividad 4: Identificación y estimación de VULNERABILIDADES:

Esta Actividad se centra en la *Vulnerabilidad*, característica conjunta de la Amenaza y el Activo (o propiedad de su relación, según se prefiera y convenga al análisis) que puede considerarse como la potencialidad o 'cercanía' previsible de la materialización de la Amenaza en Agresión. Se evalúa la vulnerabilidad como la frecuencia de ocurrencia de la amenaza sobre el activo correspondiente.

Tarea 1: Identificar vulnerabilidades.- Identificar y establecer las vulnerabilidades como relaciones entre los activos y sus amenazas, de forma individual o agrupada, a partir de las clasificaciones realizadas en las tareas anteriores. Considera tres tipos de vulnerabilidad:

- ***vulnerabilidad intrínseca****,* si no incluye ninguna salvaguarda (fuera de las naturales o implícitamente incorporadas en el activo considerado).
- ***vulnerabilidad efectiva****,* resultante de la aplicación de las salvaguardas existentes.
- ***vulnerabilidad residual,*** resultante de aplicar las salvaguardas complementarias, aconsejadas como resultado del Análisis y Gestión de Riesgos.

Actividad 5: Identificación y valoración de IMPACTOS

El objetivo de esta actividad es conocer el alcance del daño producido en el Dominio como consecuencia de la materialización de amenazas sobre los activos. El Impacto**,** visto como característica del Activo que recoge el cambio de estado de su seguridad, permite apreciar la 'gravedad' de la consecuencia generada por la Agresión, en forma de reducción de niveles de los subestados de seguridad (ACID) del Activo afectado.

Tarea 1: Identificar impactos.- Identifica el Impacto como resultado de la agresión de una amenaza a un activo, en forma de degradación de valor, de necesidad de reposición (con su coste) o de reducción de los niveles de uno o varios subestados de seguridad ACID.

Atendiendo a las dependencias entre activos, la tarea considera si el Impacto o degradación provocados en un activo pueden producir otros Impactos o degradaciones indirectas en otros activos dependientes y/o aumentar la vulnerabilidad de dichos activos dependientes frente a nuevas amenazas.

Tarea 2: Tipificar impactos.- Permite clasificar los impactos por el tipo de consecuencias que las amenazas pueden producir en los activos impactados (recogidas en el Submodelo de elementos):

- ***Impactos con consecuencias cuantitativas***
  - N1: Pérdidas económicas
  - N2: Pérdidas inmateriales
  - N3: Responsabilidad legal, civil o penal
- ***Impactos con consecuencias cualitativas orgánicas***
  - L1: Pérdida de fondos patrimoniales
  - L2. Incumplimiento de obligaciones legales
  - L3. Perturbación o situación embarazosa político-administrativa
  - L4. Daño a las personas
- ***Impactos con consecuencias cualitativas funcionales (reducción de Subestados)***
  - SA. Autenticación
  - SC. Confidencialidad
  - SI. Integridad
  - SD. Disponibilidad

Actividad 6: Evaluación del riesgo

Las informaciones sobre vulnerabilidad e impacto obtenidas en las Actividades anteriores permiten que esta Actividad establezca y estime los distintos tipos de riesgo. Esto se puede ver con facilidad cuando se representa el riesgo con la sencilla técnica matricial, como se verá de inmediato. En esta técnica se relacionan los niveles de Vulnerabilidad (puestos en filas) y los de Impacto (puestos en columnas). En las casillas correspondientes, los valores del nivel de Riesgo, como es lógico, son crecientes con los niveles de ambos factores, pero serán sistemáticamente mayores por encima de la diagonal, pues se considera que el Impacto influye más en el nivel de Riesgo que la Vulnerabilidad.

Tarea 1: Analizar las funciones de salvaguarda existentes.- Identificar las Funciones de salvaguarda actualmente implantadas en el Activo, a partir de los mecanismos de salvaguarda existentes detectados en tareas anteriores y evaluando el grado de implantación de las funciones para estimar su efectividad

Tarea 2: Evaluar el riesgo efectivo.- Calcular el riesgo efectivo, teniendo ahora en consideración las funciones de salvaguarda existentes detectadas con ayuda de la tarea previa. De estas funciones de salvaguarda, unas reducen la frecuencia de ocurrencia de la amenaza (disminución de la vulnerabilidad) y otras reducen el impacto. Los nuevos niveles actuales de vulnerabilidad y de impacto se identifican y estiman rehaciendo el procedimiento establecido por las Actividades de 'Identificación y estimación de VULNERABILIDADES' e 'Identificación y valoración de IMPACTOS' de esta misma Etapa.

1.8.1.3. Etapa 3. Gestión de riesgos

Objetivo: La Etapa permite identificar las posibles funciones o servicios de salvaguarda reductores del riesgo detectado; seleccionar las salvaguardas aceptables en función de las ya existentes y de las restricciones; simular diversas combinaciones; y especificar las finalmente elegidas, Los puntos de partida para esta etapa están constituidos por la documentación de la etapa anterior, referida a la descripción de los componentes del riesgo (activos, funciones y mecanismos de

salvaguarda existentes, amenazas, vulnerabilidades e impactos), a los niveles de riesgos calculados y a los umbrales de riesgo aceptados por el comité director.

Actividad 1: Interpretación del riesgo

Los puntos de partida para esta Actividad están constituidos por la documentación de la Etapa anterior que describe los componentes del riesgo (activos, funciones y mecanismos de salvaguarda existentes, amenazas, vulnerabilidades e impactos) y los niveles de riesgos calculados.

Tarea única: Interpretar y manejar los riesgos.- Los resultados del cálculo del riesgo intrínseco y efectivo deben interpretarse antes de poder utilizarlos, agrupándolos si cabe con objeto de identificar las áreas de mayor riesgo, del Dominio y por lo tanto las que necesitan mayor protección. Así,

- El umbral de riesgo es un valor establecido como base para decidir por comparación con él si el Riesgo efectivo calculado es asumible o aceptable*.* Los *umbrales de riesgo* utilizados pueden proceder de una estimación inicial, ratificada por la decisión del Comité director y propuesta por similitud respecto a otros casos. Estos umbrales de riesgo se pueden refinar por aplicación del Análisis y Gestión de Riesgos en un escenario de simulación del equilibrio entre los costes de los riesgos y los de las salvaguardas en un entorno de ciertas restricciones (de misión de la Organización o de su capacidad presupuestaria a corto plazo, por ejemplo).
- Mientras que el *Riesgo efectivo* calculado se considere *no asumible, Se* propone desarrollar las Actividades siguientes de '*Identificación, estimación de efectividad y Selección de las funciones de salvaguarda'* de esta Etapa.
- Cuando el *Riesgo efectivo* calculado ya se considera *asumible,* quedará como riesgo residual.

La tarea también procede a la obtención de indicadores estadísticos sobre frecuencias de ocurrencia de amenazas (vulnerabilidad), amenazas con mayor impacto, áreas más afectadas por mayores riesgos, etc.

Actividad 2: Identificación y estimación de funciones y servicios de salvaguarda

Permite identificar las funciones o servicios de salvaguarda que reducen el riesgo, así como estimar su eficacia para lograr dicha reducción.

Tarea 1: Identificar funciones y servicios de salvaguardas.- La tarea propone, sin tomar en consideración ninguna restricción, una lista de las funciones o servicios de salvaguarda que pueden reducir el riesgo superior. Las funciones o servicios propuestos se determinan con ayuda de las agrupaciones de activos/amenazas donde se detecta mayor riesgo. La organización o clasificación de las funciones y servicios de salvaguarda se apoyan en las tipologías vistas en el Submodelo de Elementos: de activos o grupos de activos (entorno, sistema de información, información, funcionalidad, otros), de amenazas (accidentes, errores, intencionales presénciales, intencionales teleactuadas) por la propia funcionalidad de las funciones y servicios (orientados a: detección, disuasión, prevención, corrección, recuperación, concienciación/información).

La lista contiene la descripción de las características de la función o activo de salvaguarda, por ejemplo: tipo de amenaza, tipo de activo que protegen, a qué subestado de seguridad (A-C-I-D) se orientan, resultado (disminución de vulnerabilidad o bien de impacto), etc.

Tarea 2: Estimar la efectividad de las funciones y servicios de salvaguarda.- A partir de la lista de funciones y servicios de salvaguarda especificados para los subdominios seleccionados del proyecto, esta tarea procede a estimar su efectividad en la reducción de los elementos integrantes del riesgo (vulnerabilidad e impacto).

Actividad 3: Selección de Funciones y Servicios de Salvaguarda

La Actividad permite seleccionar las funciones o servicios de salvaguarda convenientes y justificados como proporcionados a los riesgos que deben cubrir e incluso como óptimos.

Tarea 1: Aplicar los parámetros de selección.- Partiendo de la lista de funciones y servicios de salvaguarda propuestos, y teniendo en cuenta los

umbrales de riesgo máximo asumible o aceptable obtenidos en tareas y decisiones anteriores, la tarea ordena la lista según su efectividad para reducir el riesgo. La tarea selecciona en el orden establecido las funciones o servicios que reducen el riesgo hasta los umbrales requeridos por el objetivo de seguridad establecido.

Tarea 2: Reevaluar el riesgo.- Aplicar las funciones y servicios de salvaguarda seleccionados a la reducción de la frecuencia de ocurrencia de la amenaza (disminución de la vulnerabilidad) y a la reducción del impacto. Los nuevos niveles de vulnerabilidad y de impacto se identifican y estiman rehaciendo el procedimiento establecido por las Actividades '*Identificación y estimación de VULNERABILIDADES'* e '*Identificación y valoración de IMPACTOS'*. Los nuevos niveles de vulnerabilidad y de impacto permiten calcular el *riesgo efectivo* aplicando la misma forma anterior de evaluación del riesgo presentada en la tarea única la Actividad 1. Este valor del riesgo efectivo calculado se ha de guardar, pues será el riesgo residual si en la Actividad 9 siguiente se alcanza el cumplimiento de objetivos del proyecto de Análisis y Gestión de Riesgos.

Actividad 3: Cumplimiento de objetivos

La actividad explora si los riesgos efectivos obtenidos por la aplicación sucesiva de las funciones y servicios de salvaguarda seleccionados se encuentran bajo los umbrales de riesgo elegidos.

Tarea única: Determinar el cumplimiento de los objetivos.- Si los riesgos efectivos calculados en la tarea anterior no cumplen los objetivos de su reducción por debajo de los umbrales de riesgo fijados, la tarea organiza

- la conservación provisional de los resultados parciales alcanzados (puede haber 'retrocesos' en este proceso de simulación);
- la repetición de toda la Actividad 8 de Selección de las funciones y servicios de salvaguarda, o sea de las tareas de reconsiderar la selección y reevaluar el riesgo, antes de recomprobar el cumplimiento de los objetivos con esta tarea.

1.8.1.4. Etapa 4: Selección de salvaguardas

Objetivo.- La Etapa tiene como Objetivo la Selección de los mecanismos de salvaguarda que materialicen las funciones y servicios de salvaguarda, respeten las restricciones y reduzcan los riesgos por debajo de los umbrales deseados.

Esta etapa parte de los resultados de las etapas anteriores:

- Identificación de los mecanismos o servicios de salvaguarda que cubren, así como el grado de su implantación.
- funciones y servicios de salvaguarda seleccionados, capaces de reducir el riesgo hasta alcanzar los umbrales previamente elegidos (o bien actualizados, si se ha visto su necesidad).

Actividad 1: Identificación de mecanismos de salvaguarda

Tras seleccionar en la etapa anterior las Funciones y Servicios de salvaguarda capaces de mantener los riesgos bajo los umbrales elegidos, esta Actividad procede a identificar y analizar los posibles mecanismos de salvaguarda que materialicen las mencionadas funciones.

Tarea 1: Identificar mecanismos posibles.- La tarea procede a confeccionar una lista inicial de posibles mecanismos de salvaguarda que materialicen las funciones y servicios de salvaguarda elegidos, parte de dichas funciones y servicios de salvaguarda. Estos, habitualmente asociados a impactos y vulnerabilidades de los activos ante las amenazas, permiten identificar un conjunto de mecanismos de salvaguarda posibles.

En esta tarea no se tiene en cuenta aún el análisis del coste, efectividad, necesidades de mantenimiento, etc. de los mecanismos posibles para materializar las funciones y servicios de salvaguarda.

Tarea 2: Estudiar mecanismos implantados.- Algunos de los mecanismos de salvaguarda identificados por la tarea anterior pueden estar ya implantados en el Dominio en estudio. Esta tarea recupera la información obtenida en la recogida

de datos del Dominio que identificaba los mecanismos ya implantados y sus características. Estos mecanismos se agrupan en dos bloques:

- mecanismos coincidentes con alguno de los contenidos en la lista de mecanismos potenciales confeccionada en la tarea anterior
- mecanismos no incluidos en dicha lista

Los mecanismos incluidos en ambos bloques se analizan según diversos criterios:

- su grado de implantación,
- los costes tanto de su implantación inicial como de su mantenimiento su efectividad.

Tarea 3: Incorporar restricciones.- Se formaliza las restricciones identificadas en las actividades de recogida de información de la Etapa 1. Asimismo el Comité Director puede haber modificado el conjunto de restricciones como consecuencia de los resultados de la Etapa 2 de Análisis de Riesgos. Para incorporar las restricciones al Análisis y Gestión de Riesgos, se respeta su agrupación por distintos conceptos. En esta tarea se recoge la misma clasificación de restricciones en 6 grupos de la Etapa 1: temporales, financieras, técnicas, sociológicas, del entorno, legales.

Actividad 2: Selección de mecanismos de salvaguarda

Esta Actividad permite identificar y seleccionar los mecanismos a implantar, considerando las restricciones detectadas e incorporadas en la tarea anterior. Los mecanismos identificados y seleccionados provisionalmente se estudian en cuanto a su efectividad reductora del riesgo. Esta Actividad es iterativa, pues se repite tantas veces como sea necesario hasta obtener el conjunto de mecanismos a implantar definitivamente.

Tarea 1: Identificar mecanismos a implantar.- Se obtiene así un nuevo conjunto de mecanismos que respeta el conjunto de restricciones sin dejar de conseguir la reducción de los niveles de riesgo al de los umbrales elegidos.

Tarea 2: Evaluar el riesgo con los mecanismos elegidos.- La tarea estudia el poder reductor del riesgo de los mecanismos elegidos, por medio de las funciones y servicios de salvaguarda que aquellos materializan.

Tarea 3: Seleccionar mecanismos a implantar.- Esta tarea marca y se selecciona para la continuación del proyecto el conjunto de mecanismos obtenido por la tarea anterior como reductora suficiente del riesgo sin dejar de someterse a las restricciones impuestas.

Actividad 3: Especificación de los mecanismos a implantar

Tarea Única: Especificar los mecanismos a implantar.- La tarea especifica para los mecanismos de salvaguarda seleccionados ciertas características importantes, como:

- tipo de mecanismo
- coste aproximado
- activos protegidos
- dependencia de y a otros mecanismos
- modalidad de implantación
- otros.

Actividad 4: Planificación de la implantación

El objetivo de esta Actividad es realizar un esbozo de planificación para la implantación de los mecanismos retenidos en las Actividades anteriores.

Tarea 1: Priorizar mecanismos.- Esta tarea ordena de manera lógica y bien estructurada los mecanismos retenidos y los encuadra en proyectos potenciales de implantación, basándose en sus interdependencias y en función de las restricciones y los niveles de riesgo aceptados. La clasificación de los mecanismos dentro de las funciones y servicios de salvaguarda favorece esta ordenación y priorización.

Tarea 2: Evaluar los recursos necesarios.- La tarea estima y evalúa la intervención de recursos, tanto humanos como materiales, que conlleva la implantación de mecanismos. La clasificación de los mecanismos por grandes tipos de recursos a movilizar (organizacionales, técnicos, materiales, financieros, etc.) favorece esta estimación y evaluación.

Tarea 3: Elaborar cronogramas tentativos.- Una vez que se han definido las acciones a realizar para la implantación de mecanismos y su plazo de implantación, esta tarea las ordena en el tiempo, obteniendo los cronogramas tentativos de implantación de los mecanismos.

Actividad 5: Integración de resultados

Tarea única: Integrar los resultados.- Esta última Actividad recopila los informes producidos en las diversas Etapas y Actividades del proyecto, para confeccionar el "Informe final del Análisis y Gestión de Riesgos". La tarea también realiza los documentos de presentación de los resultados del proyecto, resultados dirigidos en unos casos a los niveles directivos y en otros a los usuarios afectados por el proyecto de Análisis y Gestión de Riesgos.

II. REVISION Y ANÁLISIS DE LOS PROCESOS EN OMNES LTD

2.1. INTRODUCCIÓN

En este capitulo el autor de la tesis tuvo como objetivo recolectar toda la información que sea posible, para lo cual se utilizó técnicas ya conocidas para la toma de información como son las entrevista, bibliografía que posee la misma empresa, y la observación de campo, que son principalmente las indicadas y las más idóneas para el desarrollo del proyecto, se encuestaron y entrevistaron a varias personas “trabajadores de la empresa” para un posterior análisis cualitativo basado en la experiencia y en opiniones de los particulares. Los procesos informales e intuitivos suelen ser más atractivos para la gerencia que los procesos estadísticos y de modelado, la base de las entrevistas y encuestas tuvieron como objetivo, la identificación de registros vitales, procesos y la identificación de las áreas funcionales (departamentos).

Se debe entender por registro vital, que es la información base de la empresa que tiene el grado catastrófico si ésta llegase a dañarse, diseminarse, o perderse, que llevaría a la empresa que comienzan con pérdidas en ventas o ingresos, ganancias, incluso de personal, tendría también la imposibilidad de cubrir requerimientos o leyes gubernamentales, de servir a los clientes, de mantener el crecimiento, de operar efectiva y eficientemente, de competir exitosamente con nuevos clientes, de mantenerse a la delantera de la competencia, de controlar los costos, y de controlar a empleados en actividades ilegales con aprovisionamiento de software, es decir un completo fracaso de la compañía con la destrucción de la información de los registros vitales.

Los registros vitales pueden estar retenidos en papel o en medios magnéticos. Algunas dependencias gubernamentales exigen a todas las organizaciones el contar con ciertos registros sin importar el medio de almacenamiento para propósitos de evidencia y/o referencia. Esto incluye registros de pago de

impuestos, nómina, pólizas de seguro, gastos, órdenes de venta por mencionar algunos. La organización podría pagar multas cuantiosas si no contase con dichos registros. Es de interés del autor el conocer las prácticas, tanto de retención como de disposición de registros vitales debido a que afectan a la seguridad y confidencialidad, así como la posibilidad de la empresa de reanudar actividades en caso de un desastre informático.

Las áreas funcionales son los departamentos que integran la compañía, el como operan es fundamental, para tener una visión más amplia de la organización del como se encuentra organizada y conocer cuales son las áreas críticas en caso de un desastre, los procesos se lograrán identificar en forma paralela a lo que se identifiquen las áreas funcionales ya que vienen a ser las actividades que se desarrollan en dichas áreas ó por personas que integran dicho departamento, es primordial identificar los procesos ya que inciden de manera directa sobre los registros vitales.

2.2. OMNES

2.2.1. Referencia Histórica

Omnes se inicio en Francia, posteriormente sus acciones fueron compradas por Schlumberger convirtiéndose en una empresa internacional de comunicaciones, siendo su misión proveer de soluciones en comunicación a las compañías multinacionales y nacionales. Inicialmente ha concentrado sus esfuerzos en el sector de exploración y producción de la industria petrolera, su visión es extender paulatinamente sus servicios a las industrias energéticas, eléctricas, mineras, químicas y al sector bancario.

Omnes por ser una compañía internacional se encuentra segmentada estratégicamente. Omnes Ecuador comparte con su similar de Colombia y Perú, funciones de carácter administrativo, organizacional y económico, la compañía se encuentra ubicada en el sector norte de Quito en las calles República del Salvador e Irlanda en el quinto piso edificio Siglo XXI, lugar donde opera el grupo Schlumberger Ecuador.

2.1.1. Funcionalidad

Omnes proporciona servicios de comunicaciones con valor agregado, ofreciendo una gama completa de servicios de red, que incluyen servicios de Internet y Mensajería, servicios de consultoría para la definición, diseño e implementación de Intranets exitosas, servicios de acceso y puesta en marcha de Extranets y servicios de instalación y puesta en marcha de redes LAN Y WAN, entre otros.

Posee una infraestructura global de comunicaciones que satisface todas las necesidades de comunicaciones y más recientemente de “outsourcing” de servicios ligados al mundo del Internet. Omnes se encuentra ubicada en todas las regiones del mundo incluyendo Europa, el Pacifico, Africa, la Comunidad de Estados Independientes y Latinoamérica (cuya sede se encuentra en Venezuela).

El mercado exige soluciones globales para satisfacer requisitos específicos. Omnes proporciona estas soluciones adaptadas a las necesidades locales, permitiendo a los clientes disponer de servicios uniformes de comunicaciones en todas sus locaciones. Aún en países lejanos, Omnes puede suministrar una gran gama de servicios competitivos, conectando lugares remotos entre si y proporcionando servicios en aquellos lugares donde sus clientes necesitan hacer negocios.

Omnes percibe la necesidad que tiene toda compañía de comunicarse interna y externamente con su cadena de proveedores; en el caso de compañías multinacionales y/o compañías ubicadas en países en vías de desarrollo, esto puede resultar excepcionalmente difícil. En este sentido, Omnes proporciona soluciones de comunicación que le permiten crear organizaciones virtuales a través de límites geográficos y estructurales, trabajando en colaboración con grupos de compañías, en zonas geográficamente definidas, para asegurar comunicaciones rápidas y confiables entre dichas compañías y su comunidad de interés.

Omnes aprovecha la experiencia de sus compañías precursoras. Cada una d ellas tiene una serie de ventajas que en la actualidad, posicionan a la

Organización entre los proveedores de comunicaciones internacionales más competitivo.

2.3. LEVANTAMIENTO REGISTROS VITALES

Los registros vitales es la información necesaria que la compañía necesita para sobrevenir de una catástrofe o de una contingencia "En Seguridad de Información", para lo cual el autor utilizó como instrumento de recolección de información el cuestionario(anexo 1), éste se aplicó desde 20 de Noviembre al 4 de Diciembre del año 2002, para lo cual cabe señalar que no hubo el apoyo necesario por parte de los trabajadores de la empresa, por lo tanto se tomó un solo representante por puesto de trabajo.

Algunos registros vitales se encuentran comúnmente en papel que son las Requisición de Compras,, Ordenes de compra, Pedidos del cliente, Facturas, Hojas de datos de cliente, que generalmente pertenecen al departamento de Compras o de Contabilidad, cuya función es hacer pedidos de materias primas y suministros necesarios. El Asistente administrativo de este departamento es responsable de garantizar que los artículos pedidos reúnan los estándares de calidad establecidos por la compañía, que se adquieran al precio más bajo y se despachen a tiempo.

A continuación se detallará los registros vitales antes mencionados:

Requisición de compras, una requisición de compra es una solicitud escrita que usualmente se envía para informar al departamento de compras, acerca de una necesidad de materiales o suministros. El procedimiento es el siguiente, el empleado llena un formato de requisición de compra y lo envía al departamento de compras para que puedan solicitar los artículos. Una requisición de compra incluye: número de la requisición, nombre del departamento o persona que hace la solicitud, cantidad de artículos solicitados, identificación del número de catalogo, costos relacionados, costo total de toda la requisición, fecha de pedido, fecha de entrega requerida y firma autorizada.

Orden de Compra*,* Sí la requisición de compra está correctamente elaborada, el departamento administrativo emitirá una orden de compra. Una orden de compra es una solicitud escrita a un proveedor, por determinados artículos a un precio convenido. La solicitud también especifica los términos de pago y de entrega. La orden de compra es la autorización al proveedor para entregar los artículos y presentar una factura. Todos los artículos comprados por la compañía deben acompañarse de las ordenes de compra, que se enumeran en serie con el fin de suministrar control sobre su uso, se incluyen los siguientes aspectos en una orden de compra: nombre impreso y dirección de la compañía que hace el pedido, número de orden de compra, nombre y dirección del proveedor, fecha de pedido, fecha de entrega requerida, términos de entrega y de pago, cantidad de artículos solicitados, número de catálogo, descripción, precio unitario y total, costos de envío, de manejo, de seguro y relacionados, costo total de toda la orden y firma autorizada.

Facturas, Este documento tiene varios orígenes dependiendo de su finalidad o propósito comercial, la factura puede presentarse por servicios prestados siendo estos los servicios tercerizados “outsourcing”, que se cobra mensualmente a los clientes ó puede originarse por otros servicios que generalmente corresponden cuando la compañía a terminado o finalizado una obra, otro tipo de factura se presenta por la compra realizada por un bien adquirido por la compañía por lo general la factura contiene la siguiente información, número de factura, número de elementos, el detalle en donde indicar el concepto de la misma, nombre del cliente, fecha de la elaboración, ciudad en donde se la realiza, valor unitario, valor parcial, valor total, valor de IVA descontado, firma del cliente, firma de un representante de la compañía, el sello de entrega.

Hojas de Datos de clientes*,* Pedidos del Cliente en estos documentos se guarda información relacionada a proyectos que se han realizado, o se vayan a realizar como presupuestos presentados para la realización de un determinado proyecto esta información se encuentra clasificada como confidencial de acuerdo a las políticas que mantiene la compañía a la cual solo personal autorizado tiene acceso.

Existen adicionalmente de los registros vitales en documentos, los registros vitales electrónicos que son los que pueden estar almacenados de forma electromagnética en discos duros, CD, floppys, cintas, estos registros son los siguientes: Archivos maestros de transacciones, archivos de referencia, archivos históricos, etc. (de bases de datos o no).

Archivos maestros de transacciones, generalmente dentro de la contabilidad de una empresa se ha vuelto imprescindible el uso de la computadora y con ello el uso de paquetes de contabilidad “aplicaciones” , dando origen a archivos de transacciones que guardan datos imprescindibles para una empresa, estratégicos y automatizados, como son el balance general de la empresa, balance mensual, roles de pago, documentos de presupuestos para clientes, documentos de control de calidad, documentos relacionados a la distribución de personal, etc.

Archivos de referencia, estos archivos son básicamente documentos escritos bajo un procesador de palabras, estos documentos pueden ser memorando, cartas de licitación, contratos, etc.

Archivos históricos, Estos archivos contienen información que llevan un orden cronológico especial, es información que guarda estrecha congruencia, y dependencia de datos actuales con datos futuros, que no pueden ser eliminados hasta que no hayan perdido su grado de importancia para una empresa, y que la perdida de la misma no perjudique a los intereses comerciales de la compañía o en la realización de un negocio, estos datos generalmente se encuentran en una base de datos.

2.4. ANÁLISIS DE REGISTROS VITALES

De acuerdo a la información recolectada en la empresa encontramos los siguientes registros vitales que pertenecen al grupo de registros impresos, el análisis de los registros vitales es primordial debido a que determinaremos de que manera se encuentran constituidos, cuales son y cual sería su impacto para la empresa en caso de suceder un desastre o de ser utilizados para otras causas que no van con los objetivos de la empresa, a continuación determinaremos cada

uno de ellos de acuerdo al departamento o área funcional donde se hallan ubicados.

Departamento Financiero: Este departamento se encarga del área de contabilidad de la empresa la misma reporta mensualmente a Omnes de Colombia todos los balances o estados de situación financiera de la empresa en el Ecuador, en este departamento tenemos o se encuentran los siguientes registros vitales: Roles de Pago, Estado financieros, Facturas de pago, Facturas por cobrar por Servicios prestados, Documentos de presupuesto de los clientes, Documentos de control de calidad del servicio prestado y telecomunicaciones de la compañía, y documentos relacionados a la distribución de personal; a pesar que estos documentos se encuentran respaldados electrónicamente es decir estos archivos se encuentran almacenados en el servidor (NT), de la compañía si su contenido es divulgado o cae en manos de competidores puede causar un incidente de grado moderado para lo cual los empleados tienen que regirse a las normas, políticas y procedimientos que mantiene la empresa para medios removibles de almacenamiento de información.

Departamento de Gerencia de Proyectos: Este departamento tiene a su cargo la continuidad del negocio con los clientes existentes y captar nuevos clientes, para lo cual se encarga de desarrollar documentos que contienen estrategias de mercadeo o información relacionada a productos o servicios que la compañía promociona y promueve dentro de la industria petrolera, en este departamento podemos identificar los siguientes registros vitales:

Control de calidad de proyectos especiales, Documentos de resultados después de haber hechos análisis de productos y documentos de implementación de proyectos, todos estos documentos además de estar impresos se encuentras almacenados en el disco del servidor1 de la compañía, el grado de impacto si el contenido de estos documentos llegara a diseminarse es de grado moderado.

Departamento de Ventas: Este departamento es dependiente del departamento de proyectos guardan una estrecha relación debido a que tienen a su cargo el desarrollo de nuevos productos y de dar el soporte técnico de un servicio o

producto en el cual tenemos los siguientes registros vitales: Documentos de presupuestos para la realización de proyectos. Este registro tiene el grado de moderado si llegará diseminarse el contenido del cualquier producto.

El departamento de Helpdesk*:* No tienen registros vitales impresos importantes que se puedan mencionar, al igual que el departamento de Gerencia y de la misma manera el departamento de Recursos Humanos debido a que los más importantes dentro de Omnes son los que ya hemos detallado con anterioridad.

Los registros vitales en forma digital son todos los archivos, como sistemas operativos, base de datos, archivos históricos, que llegan a tener información primordial o fundamental que pueden interrumpir las operaciones o labores cotidianas que realiza la compañía, cuando estos registros vitales llegan a perderse, diseminarse, o simple no funcionan. La compañía posee clientes que han depositado su confianza para que maneje sus sistemas de información podrían retirar su confianza debido a una interrupción en sus actividades comerciales por la falta de asistencia técnica, es de esta manera como se vería perjudicada la imagen de la empresa “OMNES”, cabe destacar que la empresa realiza proyectos como de cableado estructurado y Smart Cards “Tarjetas Inteligentes”, procesos que operan las 24 horas del día en las locaciones donde Omnes instalo dichos servicios, los sistemas informáticos que posee la compañía poseen información propia de la misma como también del resto de compañías que conforman el grupo Schlumberger, documentos respecto a la realización de nuevos proyectos para captar clientes, documentos de cada uno de los usuarios “Respaldos” de la compañía que se encuentra en carpetas asignados a cada uno de ellos en el servidor(NT y NT-B), para que respalden información que a criterios de ellos consideren fundamental.

En lo que corresponde a los registros vitales digitales los vamos a encontrar únicamente en el departamento de helpdesk específicamente en los discos de los servidores (NT, y NT-B) en el servidor NT realiza las funciones de correo electrónico de la empresa, es adicionalmente servidor de impresión, servidor de DNS, Almacena información de la empresa REDA (perteneciente al grupo

Schlumberger). El servidor NT-B realiza las funciones de servidor DHCP, de servidor WINS, servidor de almacenamiento de información, y mantiene una base de datos en ORACLE, la información que guarda la misma es de todo el grupo Schlumberger, como también de sus propios clientes, todos los servicios que desempeñan estos servidores tienen el grado de moderado si llegara a producirse un catástrofe informático; existen otros servidores que se encargan del control de acceso al edificio, y de control de telefonía que no los vamos a mencionar debido a que no guardan información que pueda considerarse vital para la empresa, cabe mencionar que Omnes guarda información de otras compañías del grupo Schlumberger y adicionalmente es la encargada de dar soporte técnico a las mismas, y a los clientes de Omnes, cada usuario tiene asignado una carpeta en donde puede realizar respaldos de la información crítica que posea, existe un firewall instalado en cada uno de los servidores que protegen la información que contienen, estos cortafuegos siguen un estándar riguroso al cual deben seguir para estar en funcionamiento. En cuanto a la seguridad física la máquina del cortafuego y cualquier consola de mando asociada a ésta se encuentra en el área física denominada cuarto de servidores bajo normas de precaución, dicho espacio físico cuenta con refrigeración o aire acondicionado para mantener los equipos en un nivel de temperatura normal para evitar la degradación del equipo, el acceso físico es restringido tal como determinan las normas generales de acceso a éstos. No Existe una etiqueta o letrero que debe indicarse de la siguiente manera Omnes Warning como un estandarte de advertencia que debe desplegarse para todos los usuarios que intentan acceder a dicho cuarto. Otra Norma de los Estandartes que debe seguirse es que los administradores deben guardar parches (particularmente relacionado a la seguridad) y poner al día el software del cortafuego lo más pronto posible.

El Software que contiene Omnes se encuentra respaldado en el servidor NT al cual solo puede ingresar personal de helpdesk para realizar una instalación, los discos originales se encuentran en una caja fuerte ubicada en el centro de cómputo, el software es el siguiente:

SOFTWARE	TIPO DE SOFTWARE
Microsoft Windows 2000	Sistema Operativo Estándar de la Compañía instalado en todos los computadores personales.
Microsoft Windows NT Server	Sistema Operativo de Servidores de la Compañía.
Mac OS 9	Sistema Operativo IMAC G3
Microsoft Office 2000 Standard	Suite de Procesamiento de texto electrónico y Hoja electrónica y presentaciones.
CheckPoint 4.0	Sistema para uso de Redes VPN(Redes privadas Virtuales)
Radia 2.0	Sistema de Inventario de Hardware y Software vía Internet
Oracle 8.0	Base de datos Oficial de Omnes Trabaja con Siebel 3.1
Siebel 3.1	Sistema de mercadeo e inventarios cuya base de datos se encuentra en Bruselas
Kery 2.0	Sistema de control de acceso a los pisos y de activación de alarmas
Eudora Pro 5.1	Sistema de Correspondencia electrónica
Mcafee Virus Scan 4.5	Sistema de Detección de Virus

Tabla 2-1: Software Base de la Compañía

SOFTWARE	TIPO DE SOFTWARE
SAP Basis	Sistema para manejo de Recursos Humanos
SAFIWIN	Sistema Administrativo Financiero Integrado
Intermapper 2.0	Sistema de control y monitoreo de en enlaces satelitales, programable por el usuario.

SOFTWARE	TIPO DE SOFTWARE
KEOPS	Sistema de Contabilidad

Tabla 2-2: Software de Aplicación para Servidores y Computadores Personales.

2.5. PRINCIPALES POLÍTICAS Y PRÁCTICAS OBLIGATORIAS PARA EL PERSONAL DE OMNES

Dentro de las principales políticas y reglas que el personal debe poner en práctica dentro de sus labores cotidianas tenemos la principal y más importante lo que se denomina TOP 12 que son 12 puntos que a continuación las detallamos:

2.5.1. Actualización del Registro Laboral

Los empleados es el recurso más importante de Omnes. El directorio proporciona una manera eficaz de localizarlos. Cada empleado tiene una cuenta en el directorio. La información guardada en esta cuenta es conocida como su registro laboral. Hay muchas personas a lo largo de la compañía que están autorizadas para crear las cuentas, dar soporte técnico, o restablecer las contraseñas. Estas personas son llamadas Administradores de directorio, expertos y dominantes en el área de soporte técnico. Aunque alguna información en su registro es controlada por la sincronización con otra base de datos (por ejemplo, la información de su cargo se toma de la base de datos de SAP/BASIS de Personal), el empleado es el encargado de actualizar la mayoría de su información de su registro laboral, cuando exista alguna modificación como por ejemplo cuando cambio de lugar de trabajo “Ciudad”.

Para realizar los pasos siguientes el trabajador se conectará a la Intranet de Omnes para acceder a los enlaces siguientes.

TAREA	PROCEDIMIENTO A SEGUIR
1. Pida una	Localice a un trabajador de helpdesk más cercano. Su

TAREA	PROCEDIMIENTO A SEGUIR
cuenta del directorio si usted no tiene una.	gerente o departamento de personal debe autorizar su petición para una cuenta de directorio.
2. Repase la exactitud de su registro actual.	Realice una consulta a la base de datos de directorios (http://directory.slb.com/query.cgi). Ingrese su nombre, y desde el menú desplegable de la página elija **Request Subset**, para ver todos los atributos del registro.
3. Cuando sea necesario, ponga al día su registro.	Ingresar su usuario y clave en el Web para ingresar a la página (http://directory.slb.com/update-record.cgi) para proceder a la actualización. Usted debe saber su contraseña para poder ingresar. Si usted se olvidó de su contraseña, contáctese con un funcionario de helpdesk.
4. Cambie su contraseña.	Ingrese el formulario de actualización en el Web (http://directory.slb.com/update-record.cgi?menu=password) y seleccione del menú desplegable la opción de actualización de contraseña. Se otorga a las nuevas cuentas contraseñas predefinidas que son débiles que el usuario debe restablecer inmediatamente después que se le creo su cuenta. Usted puede necesitar cambiar su contraseña en otros momentos. Siempre seleccione muy bien las contraseñas (http://security.slb.com/training/users/passwords.html).

Tabla 2-3: Procedimiento de Actualización del Registro Laboral

2.5.2. Protección de la información del Cliente

La reputación de Omnes con los clientes se construye a través de la confianza. La protección pobre de datos del cliente podría llevar a la pérdida de clientes si los datos terminan en las manos de un competidor. La Seguridad de la información se compromete en evitar la divulgación, alteración, o pérdida de la misma. La mayoría de los problemas es debido al error humano, crímenes por computadora, se debe permitir que los clientes intervengan en la seguridad de sus datos.

Use los siguientes procedimientos para ocuparse de los datos del cliente en forma correcta.

TIPO DE DATOS	PRÁCTICA ADECUADA
Correo electrónico	No enviar correo en forma automática. Esto puede evitar el envío de información de propiedad de Omnes de manera inadvertida a direcciones de correo electrónico fuera del cortafuego de Omnes
Datasets	1) los permisos de archivo deben configurarse para un acceso mínimo y necesario; sólo aquellos individuos que lo necesitan deben ser capaces de ver los datos específicos del cliente. 2) Los respaldos de los datos deben ser almacenados en un lugar seguro. 3) Los datasets del cliente usados para pruebas internas deben ser saneados para prevenir el descubrimiento (por ejemplo eliminar nombres, locaciones, direcciones API).
La Información de terceras personas es cubierto por el acuerdo de falta de revelación de	No anunciar esta información en páginas Web de la Intranet o en boletines de anuncios.

TIPO DE DATOS	PRÁCTICA ADECUADA
hechos	

Figura 2-4: Modos de Protección de la Información.

2.5.3. Computadoras desatendidas

Las computadoras que se encuentran encendidas y que no existe nadie quien las utilice siempre se las considerará un riesgo. La mayoría de brechas en seguridad de computación informadas son cometidas por personas que han manipulado el computador de manera directa esto es sentándose en frente del mismo, es decir, por alguien que no está autorizado pero que tiene acceso físico. Estas personas podrían ser internos, contratistas, consultores, clientes, visitantes, o vendedores. La pérdida de información no puede ser intencional; puede causarse inadvertidamente por la negligencia, mal uso, o falta de conocimiento. Pero el resultado final es muy costoso. Las computadoras que son de alto riesgo al acceso físico desautorizado son aquellos localizadas en lugares públicos, los empleados que se encuentren viajando, o a su vez en instalaciones ajenas a la compañía deben tomar dicha precaución:

- Riesgo alto: aeropuertos, vehículos, medios compartidos (como las situaciones en el campo), oficinas del cliente
- Riesgo moderado: los cubículos, las estaciones de secretarias, las oficinas de Omnes.

Una persona con acceso físico a su computadora puede enviar correo electrónico con archivos desde su computadora a locaciones externas, aun cuando ellos no conozcan su contraseña de correo electrónico.

Aunque apague su máquina debe mantenerla lejos del alcance de usuarios desautorizados, también debe prevenir que se acerquen a su computadora a pedir algún tipo de ayuda. Para ello, active su protector de pantalla protegido por contraseña.

ÁREA A SER PROTEGIDA	QUE HACER
Alto Riesgo - Aeropuertos, Vehículos, Medios compartidos (situaciones de trabajo en el campo), oficinas del cliente	1. Configurar las computadoras con contraseña al momento que se inician. 2. Usar protector de pantalla con petición de contraseña que se active después de 5 minutos. 3. Use cables blindados y seguros siempre que sea posible, por ejemplo en las oficinas del cliente y situaciones de trabajo en el campo. 4. No colocar la maleta de la computadora en la cajuela de un TAXI. 5. Si usted está en un hotel, desconecte y ponga su computadora en una maleta cerrada con llave o en la caja fuerte de alquiler del hotel. 6. Nunca asuma que usted es inmune al acceso físico desautorizado. 7. No incluya las computadoras portátiles a prechequeo de carga cuando vaya a volar, siempre debe estar en una maleta cerrada con llave.
Riesgo moderado: - cubículos, las estaciones de secretarias, las oficinas de Omnes.	1. Asegurar el equipo vía cables seguros con llave para prevenir que sean robados. 2. Usar un protector de pantalla

ÁREA A SER PROTEGIDA	QUE HACER
	activado con contraseña que se activará después de 5 minutos. 3. Aun cuando usted tenga una oficina cerrada con llave, nunca asuma que usted es inmune al acceso físico desautorizado.

Figura 2-5: Áreas a ser protegidas.

2.5.4. El protector de pantalla activado con contraseña

Todas las computadoras personales pueden y deben ser protegidos con una clave en el protector de pantalla. Un protector de pantalla es una imagen animada desplegada en la pantalla del monitor para prevenir un mayor desgaste del fósforo de la pantalla. Como una medida de seguridad, un protector de pantalla puede activársele con una contraseña para que nadie pueda acceder a su computadora mientras usted está lejos. El protector de pantalla debe activarse después de un lapso de 5 minutos y activarse por el movimiento del ratón o el teclado. Un protector de pantalla protegido por contraseña detiene a los usuarios desautorizados.

Un protector de pantalla protegido por contraseña es la primera línea de defensa contra la pérdida de información.

Modo de activar un protector de pantalla protegido por contraseña en su computadora:

PLATAFORMA	PRACTICA RECOMENDADA
Windows 95, NT,	1. En la barra de tareas, haga clic botón Inicio. 2. Seleccione **configuración -> Panel de Control**

PLATAFORMA	PRACTICA RECOMENDADA
	menú opciones. Abra la ventana del Panel de control. 3. Seleccione la opción de Desplegar. Abra la ventana de Propiedades de Desplegar. 4. Haga clic en la etiqueta protector de Pantalla. 5. Seleccione la caja de dialogo protegido por Contraseña 6. Ponga el tiempo de espera de 5 minutos 7. Pulse el botón OK para aplicar los cambios.
Macintosh	El software de protector de pantalla, After Dark 4.0.3, tiene el mecanismo de una protección de contraseña razonable que es activado cuando el protector de pantalla se activa y cuando la máquina se enciende. Este software trabaja con todas las versiones de MacOS, de 7.1 a 8.0. la actualización de After Dark 4.0.3 es gratis. Cuando usted ejecuta el updater, se instala el motor de After Dark y dos protectores de pantalla (la pantalla oscura y la Noche Estrellada), aun cuando su máquina no lo haya tenido instalado. Este software está aprobado por el equipo de helpdesk de Omnes.

Figura 2-6: Modo de habilitar protector de pantalla.

2.5.5. Realizar respaldos de manera regular

Los archivos de datos son valiosos, y deben ser respaldados rutinariamente en un medio de almacenamiento. La pérdida de datos no sólo puede llevar a la pérdida de información vital, pero el tiempo perdido (horas o días) en tratar de recuperar los archivos perdidos. La pérdida de datos puede ocurrir en las siguientes situaciones:

- archivos accidentalmente borrados de su propio computador o de una computadora de archivos compartidos
- archivos adulterados por los virus (u otro vandalismo)
- fallas de hardware
- los desastres naturales

Los respaldos protegen la información en contra del error humano que es la causa principal en la pérdida de datos.

Use la tabla siguiente para que usted se asegure que a conseguido respaldos de calidad de su sistema

QUE HACER	CÓMO HACERLO
1. Asegúrese que cuenta con alguna persona que lo pueda asesorar Nunca asuma que usted lo conoce todo. Pregunte por alguna persona de soporte de sistemas.	• **Si los respaldos automatizados de su computador están disponibles:** Usted debe realizar los respaldos de una manera segura de su sistema. Si su software de respaldo le dice que usted nunca se ha realizado respaldos o no se ha realizado respaldos por un período mayor de una semana, usted debe proceder a realizarlos. • **Si usted accede a un servidor de manera regular -** Es su responsabilidad copiar los datos críticos a este servidor durante el tiempo que usted tiene para hacerlo. • **Si no hay ningún procedimiento para realizar respaldos disponibles -** Ver el item número 2, que continúa.
2. Si no hay ningún procedimiento de	Las unidades de disco externas y de cinta magnética como unidades Jazz o cintas DAT de 4mm pueden

QUE HACER	CÓMO HACERLO
respaldo automatizado, establezca su propio procedimiento.	hacer los respaldos de manera simple y barata.
3. Verifique la integridad de respaldo.	Periódicamente cheque que usted puede leer algunos archivos que se han respaldados. Pasa muy a menudo, debido a un error en los procedimientos de respaldos, los archivos son ilegibles. Evítese las sorpresas.
4. Guarde todos los respaldos en lugares seguros, lejos de los sistemas los respaldos deben estar fuera del calor o de las fuentes magnéticas.	Vea también –Top 12: los Medios de comunicación Trasladables.

Figura 2-7: Respaldos de Información

2.5.6. Protección en contra de virus

Más de 300 nuevos virus aparecen cada mes. Más de una docena de nuevos virus se crean a diario. La mayor parte de ellos afectan a las computadoras con Windows 9x, Windows NT, Windows 2000. Las computadoras Macintosh también deberían ser protegidas, en parte para prevenir el avance de virus de PC. Las máquinas de Unix que almacenan archivos de PC o Macintosh también necesitan ser supervisadas, pero esto se maneja típicamente por administradores del sistema.

Los virus de computadoras son programas (ejecutables) que causan daño a la computadora y se extiende a otros sistemas, normalmente vía archivos por correo electrónico. Los archivos ejecutables a veces pueden ser identificados por el tipo de archivo (extensión de archivo. EXT. VBS. LNK, o el SCRIPT.INI son los más comunes). Los documentos de texto plano no pueden contener virus. Sin embargo, los documentos generados en Microsoft Word y Excel (.xls, .xlt, .doc) contienen texto y código ejecutable (macros), y las macros pueden contener los virus. Los virus permanecen inactivos y no pueden extenderse o dañarse hasta que no se ejecuten, o en el caso de virus de macros, hasta que el archivo sea abierto. Hay un gran aumento de macro virus, porque ellos son relativamente fáciles de crear y los documentos que los contienen son extensamente distribuidos. El daño de virus puede ser inocuo o muy destructivo. Aquí hay una lista de algunos cosas que los virus pueden realizar:

- cambian el contenido de los documentos de texto y los programas ejecutables
- borran archivos
- borran contraseñas (dejando a la computadora vulnerable a otros ataques)
- insertan líneas dañinas de código en archivos de instalación, deshabilitando totalmente a la computadora ante un ataque.

Sólo usted puede prevenir el avance de virus. Mantenga su protección de virus a corriente y aprende a descubrir nuevos virus que incluso son desconocidos para las última herramientas de antivirus.

Siga estos procedimientos para proteger los datos de los ataques de virus

QUE HACER	COMO HACERLO
1. Aprenda a identificar un virus potencial que llega por	Nunca abra un archivo ejecutable que se lo haya enviado de una fuente externa a

QUE HACER	COMO HACERLO
correo electrónico.	Omnes. Refiérase a la página de ayuda en protección de virus para los consejos en identificar un virus, siempre tenga en cuenta lo siguiente. Las herramientas de Antivirus sólo lo protegen en contra de virus conocidos, y nuevos virus aparecen todos los días.
2. Instale y configure propiamente la última herramienta del antivirus.	Refiérase a la página de ayuda de Protección de virus para instrucciones.
3. Configure las aplicaciones vulnerables como Microsoft Office, Eudora, y Microsoft Outlook para una protección máxima contra virus.	Refiérase a la página de ayuda en protección de virus para instrucciones.
4. Mantenga una protección de antivirus equivalente para las máquinas de la casa que comparten archivos con los sistemas de Omnes.	Usted puede usar el software corporativo autorizado para este propósito.
5. Informe de los virus cuando se hayan	a) Si su computador fuere infectado, siga el procedimiento de manejo de Virus.

QUE HACER	COMO HACERLO
encontrado.	b) Si un archivo ejecutable relacionado al negocio de Omnes es enviado a usted desde el interior de SINet, contéstele al creador que los ejecutables contienen a menudo código malévolo (virus), y pídale que le confirme que el código es seguro.
	c) Si usted observa prácticas inseguras dentro de Omnes, infórmeles usando el procedimiento de reporte de Riesgos (Ver Uso de la Herramienta QUEST).
6. Reparación de un daño causado por virus conocido.	Refiérase a las instrucciones para las últimas alarmas de virus.

Figura 2-8: Protección de Virus

2.5.7. Software con Licencia

El Uso de software propiamente autorizado es importante por dos razones:

Obligación legal: El Uso de software comercial sin pagar por él es ilegal. Omnes podría ser auditado por vendedores comerciales y organismos de control para verificar la autorización apropiada.

Riesgos de Software Shareware/Freeware: El software no comercial (Freeware y Shareware) puede contener código malévolo capaz de producir los siguientes daños:

- pérdida, corrupción o descubrimiento de archivos
- la creación de agujeros de seguridad que permiten el acceso desautorizado

El software comercial probablemente contenga menos código malévolo que el software shareware y freeware, que son programas de libre distribución.

La compañía paga por todo el software comercial y se mantiene dentro de los acuerdos de autorización de la licencia. La empresa impide el uso de código no comercial en la red de computadoras de Omnes.

Use estas pautas cuando use software comercial, shareware, o freeware.

TIPO DE SOFTWARE	QUE HACER
Software comercial	El software con licencia autorizado está disponible en el servidor de distribución de Software de Omnes (SDS). Otro software comercial debe ser solicitado a través de su agente de compras local. NOTA: A menos que no esté listado en la página Web de uso casero, usted no puede instalar software de la compañía en su computadora de la casa.
Shareware (software de dominio no público)	Usuarios que obtienen y usan shareware son esperados un tiempo prudencial para que envíen o se registren y retribuyan económicamente a los autores del shareware. El uso de shareware está claramente detallado en el acuerdo de licencia o en el menú opciones ->**About.** Shareware obtenido de fuentes no confiables debe probarse en computadoras aisladas, para que posibles daños sean restringidos. NOTA: Usted es responsable por cualquier daño hecho por software que usted instalo de fuentes no aprobadas.
Freeware (software de dominio público)	El freeware puede copiarse libremente y puede distribuirse sin las restricciones de una autorización y puede retribuirse.

TIPO DE SOFTWARE	QUE HACER
	Programa de libre distribución obtenido de fuentes no confiables debe probarse en computadoras aisladas, para que el posible daño sea restringido. NOTA: El usuario es responsable por cualquier daño hecho por software instalado en su PC de fuentes no aprobadas.

Figura 2-9: Tipo de Software existentes

2.5.8. Medios de almacenamiento Removibles

Dentro de los medios de comunicación trasladables también se les incluye:

- impresiones, que son documentos impresos y registros de seguimientos de archivos
- archivos electrónicos almacenados en CD-ROMs, cintas, y discos flexibles

Los medios de comunicación trasladables presentan una amenaza a la seguridad de la información porque estos artículos pueden fácilmente perderse o ser robados, a menos que la información que posean sea encriptada o estos dispositivos sean guardados en un ambiente cerrado y seguro. La falte de un proceso de inventario y de normas de clasificación en seguridad de información dificultan la administración de estos recursos. Una pérdida a menudo no es detectada.

Las normas de clasificación en seguridad de Información de Omnes describe cuatro grandes categorías: secreta, confidencial, privada, y pública. Cada una tiene las medidas de seguridad correspondientes. Las pautas proporcionadas a continuación son basadas en estas normas.

Mantener un inventario de sus recursos de medios de comunicación trasladables. Emplear medidas de seguridad apropiadas basadas en el tipo de información almacenada en los medios de comunicación trasladables.

QUE HACER	COMO HACERLO
1. Mantenga un inventario de los medios de comunicación removibles para los cuales usted será responsable.	a) Refiérase a la tabla de clasificación de seguridad de información para ejemplos y pautas en manejo y almacenamiento de información. b) Use la hoja de cálculo de inventarios c) Marque de una manera clara todos los medios de comunicación trasladables con la debida clasificación en seguridad.
2. Cuando no los esté utilizando, quítelos de su computadora todos los medios de comunicación que contienen información secreta, confidencial, o privada. Guárdelos en el lugar apropiado.	NOTA: Esto es importante hacerlo antes de transportarse con computadoras portátiles**.**
3. Destruya, y vote a la basura, todos los medios removibles de almacenamiento obsoletos.	Ver el procedimiento de destrucción de medios de almacenamiento obsoletos.

Figura 2-10 Manejo de los medios de almacenamiento

2.5.9. Destrucción de medios removibles obsoletos

El material sensible que llega a ser obsoleto puede caer en manos equivocadas. Un método, llamado "dumpster diving" está basado en la idea que si usted sabe de la basura de alguien, usted los conoce. Asegúrese que su basura no contiene

la información útil. Propiamente destruya el material obsoleto antes de disponer de él.

El material obsoleto también debe destruirse para prevenir sean usadas por equivocación y causen la realización de errores. Siempre destruya las versiones anteriores cuando las nuevas versiones son recibidas. Puede parecer improbable para usted, pero “dumpster-diving” sucede realmente dentro de una empresa.

REALIZAR TRIMESTRALMENTE
1. Identifique a su Funcionario de Seguridad de Sitio (SSO) y su administrador de medios informáticos. Indague por los procedimientos locales en cómo disponer de medios de almacenamiento.
2. Si usted necesita destruir medios de almacenamiento con información confidencial de cualquier tipo, el SSO o el Administrador de medios informáticos recogerá los medios de almacenamiento y dispondrá de ellos trimestralmente.
3. Usted puede disponer de los medios de almacenamiento con información no confidencial, que debe destruirla. • Borrando todos los datos de discos flexibles “volviendo a formatearlos”. • Destruyendo los CD de datos “rompiéndolos”. ¡PRECAUCIÓN! : ¡Tratar de romper los CD usando gafas! Cuando rompa un CD, utilice gafas de seguridad y guantes y sujete el CD dentro de un cubo de basura.
4. Siga los procedimientos locales, destruya los recursos de papel anticuados. Normalmente esto requiere el uso de una máquina diseñada para este propósito.
5. Guarde un registro de medios de comunicación destruidos en su Hoja

REALIZAR TRIMESTRALMENTE
de cálculo de Inventario.

Figura 2-11: Procedimiento de manejo de medios de almacenamiento

2.5.10. Deshabilite el modo de auto respuesta del Modem

Si su computadora tiene un módem conectado a una línea telefónica, es posible para alguien llamar a su computador. Si su módem o el software que habla con su módem está configurado para auto contestar, alguien puede tener acceso a su computador vía conexión telefónica. Qué pasa luego depende del tipo de software y hardware que usted usa. Si su software de fax contesta el módem, la llamada externa puede enviarle sólo un fax. Si un servidor de acceso remoto como un ARA, PPP, o servidor de NT contesta el módem, el intruso puede acceder al resto de computadoras en la red de Omnes “SINet” que su computador tiene acceso. Si su computadora es una máquina de Unix sin ningún programa configure el puerto del Modem para contestar, ofrecerá el modo de consola lo más probable.

¿Qué tan grande es el riesgo que se infiltren por el módem? Hay un ataque de computadora conocido como “war dialing” el cual usa el software para auto marcar números de teléfono consecutivos, se detiene solo cuando encuentra un módem que contesta la llamada. El software war-dialing es gratuito y está disponible en el Internet.

¿Cómo probar que usted tiene software de servidor ARA, PPP o NT instalado en su máquina? Esto muy probablemente no lo sea. Típicamente usted sólo tiene software de cliente que habla con estos servidores. Si usted no tuviera software para el lado del cliente, usted no podría usar su cuenta de dial up. El software del cliente no presenta un riesgo sólo el software del servidor

El software de aplicaciones puede resetear el módem para dejarlos en modo de auto contestar y obtener acceso desautorizado a la red.

Use las estrategias de contraseña seguras listadas en la siguiente tabla

QUE HACER	COMO HACERLO
1. Determine si su módem está configurado para auto contestar.	Un método fácil es llamar al número de la línea telefónica conectada al módem de su computadora: a) Si usted oye un zumbido telefónico, pero nadie contesta, el módem no está configurado para auto contestar. b) Si usted oye el sonido de fax, su módem está configurado para auto contestar pero el software que contesta es software de fax y no representa ninguna amenaza de seguridad. c) Si contesta, continúe con el paso #2. d) Si usted oye el sonido del Modem, su módem está configurado para auto contestar. Continúe con paso #2.
2. Determine qué software está configurado para recibir llamadas hechas al módem.	Si usted no está seguro que software de servidor está instalado en su computador, entonces las oportunidades de que usted lo desinstale no existen. Por favor avise a su personal auxiliar o al experto local y pídales que lo ayuden a determinar qué tipo de software de servidor está contestando sus llamadas de módem.
3. Desactive la opción de auto respuesta en el propio software.	Recuerde, el software del fax que está configurado para contestar su módem no presenta una amenaza de seguridad

Figura 2-12: Deshabilitando un modem

2.5.11. Reportando Riesgos en Seguridad

El trabajador es uno de los mejores recursos para mejorar la seguridad de la información en Omnes. Su visión en dónde los riesgos puedan existir, el impacto a los procedimientos de seguridad en los sitio locales, en donde el trabajador ha llegado a dar testimonio de cualquiera de los siguientes riesgos.

- **La pérdida de confidencialidad -** descubrimiento desautorizado o interceptación
- **La pérdida de integridad -** cambios o corrupción de información y datos
- **Acceso físico desautorizado -** a computadoras o edificios
- **Falta de disponibilidad -** Denegar servicios informáticos ó incapacidad para acceder la información
- **El error humano**
- **Los catástrofes naturales**

Los incidentes en seguridad de información son notoriamente difíciles de descubrir. Las estimaciones de la Industria indican que menos del 10% de todas las casualidades de computación son detectadas, y muy pocas reportadas. Aunque los administradores de red y sistemas vigilan los sistemas de computación, usted puede ayudar siendo consciente, reportando los incidentes sospechosas a su funcionario de seguridad de sitio, y usando el Informe de Identificación de Riesgo (RIR) para llamar la atención a los riesgos potenciales.

Rellenando un RIR no debe ser considerado un acto de reproche. Esto es simplemente una manera de traer la atención a las debilidades y ayudar a enfocar en programas y procedimientos de entrenamiento

QUE HACER	CÓMO HACERLO
1. Identifique e	Use el Informe de Identificación de Riesgo.

QUE HACER	CÓMO HACERLO
informe los riesgos de seguridad de información. Haga una revisión trimestral por lo menos a esto.	Refiérase a la Lista de control de auditoria de sitio (usado por SSO) y los módulos de entrenamiento “Top 12”. Su responsabilidad es informar algo que parece comprometer las metas de seguridad.
2. Antes de que las alarmas generales suenen, informe la actividad sospechosa a su Funcionario de Seguridad de Sitio (SSO).	Use el directorio para buscar el SSO más cercano. Las siguientes posibilidades pueden ser sólo riesgos cuando ellas existan en su extremo: • Actividad masiva en el disco. Los programas de computadoras y de red a menudo ejecutan programas que consumen recursos en la CPU mientras el usuario está ocioso, de tal manera que una computadora activa no puede implicar una brecha de computación. • Los archivos del Sistema tienen la fecha de modificación más reciente • La fecha de su último inicio de sesión (Login) es más reciente • Archivos que están extraviados, aparecen, o que a su vez su contenido a sido alterado. • Llamadas telefónicas u otros pedidos de solicitud de información para el acceso a una computadora le piden que proporcione. • Bromas por correo electrónico sospechosas. • Puertas abiertas en los medios de información

QUE HACER	CÓMO HACERLO
	seguros. • Personas no identificadas que entran en los medios seguros sin la debida identificación (por ejemplo, sin ninguna insignia de visitante).
3. Si usted posee una computadora portátil, grabe el número de etiqueta de servicio.	Cuando usted compra una computadora a través de los métodos normales de Omnes y la tiene instalado según las normas, el número de etiqueta de servicio se grabará automáticamente. Si usted no tiene una instalación normal, usted personalmente debe grabarlo para referencia aun cuando si su computadora es robada. Si su computadora es robada, haga los siguientes reportes: • Avise el departamento Policía y haga una denuncia con ellos. • Si su computadora portátil fuera un Dell (la norma corporativa actual), contacte a servicio al cliente Dell al 1-800-822-8965. Dele al representante de servicio al cliente el número de etiqueta de servicio

QUE HACER	CÓMO HACERLO
	de su máquina robada. Asegúrese que ellos hacen una nota en su boleto de servicio que el sistema fue robado. • Informe del incidente a su Funcionario de Seguridad de Sitio. Usted puede encontrarlo en la dirección "http://directory.slb.com/roles.html" haga una consulta ingrese su nombre y seleccione "SSO" del menú desplegable.

Figura 2-13: Modo de reportar un riesgo.

2.6. CLASIFICACIÓN DE LA INFORMACIÓN DE OMNES

La clasificación de la información y las medidas de seguridad correspondientes para el almacenamiento de información en medios trasladables.

CLASIFICACIÓN	INFORMACIÓN	MEDIDAS DE SEGURIDAD APROPIADAS
Secreto	W&T - Toda la información relacionada a proyectos "limitados" (que se encuentre en pruebas ENP) Marketing - Los datos del Cliente relacionados a la producción	• Las impresiones deben ser físicamente aseguradas. • La información electrónica debe encriptarse o físicamente asegurada. • El dueño de la información debe explícitamente identificar a los usuarios autorizados.

CLASIFICACIÓN	INFORMACIÓN	MEDIDAS DE SEGURIDAD APROPIADAS
		• La autenticación del usuario es requerido. • Deben marcarse como SECRETA a los medios removibles de almacenamiento. • Deben enviarse los medios de comunicación por mensajería segura.
Confidencial	Las Operaciones de campo - Manuales relacionados de mantenimiento de herramientas, administración de campo, administración de contratos, equipos de campo, cumplimiento de exportación, administración de riesgos. Los centros de R&E - Toda la información relacionada a proyectos limitados (proyectos que han empezado con pruebas de ENP) Marketing - CD ROMs con nuevos productos técnicos de entrenamiento	• Las impresiones deben estar físicamente seguras. • La información electrónica debe encriptarse o físicamente asegurada. • La información debe estar disponible en una necesidad de conocimientos de lo más básico “Resumen”. • La autenticación del usuario es requerido. • Deben marcarse los medios de almacenamiento de información como CONFIDENCIAL.

CLASIFICACIÓN	INFORMACIÓN	MEDIDAS DE SEGURIDAD APROPIADAS
	Recursos Humanos – El sueldo Individual o información de desempeño individual, Centro de capacitación en línea.	• Deben enviarse los medios de almacenamiento vía empresa de transporte comercial afianzado.
Privado	Las Operaciones de Campo – Catálogos de Equipos, manuales de referencia de Wellsite de W&T, los manuales de HSE, Control de Calidad. Centrales de R&E - Información relacionada a proyectos de acceso abierto (es decir que el proceso de comercialización ha empezado) El personal - el directorio Corporativo	• La encriptación no es necesaria. • Todos los empleados de Omnes pueden tener acceso. • Deben marcarse los medios de almacenamiento de información con la norma legal de declaración de Omnes. • Pueden enviarse los medios de almacenamiento por una empresa comercial de transporte afianzada.
Público	Operaciones de campo - manuales de los Clientes Los Centros de R&E - la Información relacionada a los productos comercializados Folletos de Reclutamiento	Ninguna restricción

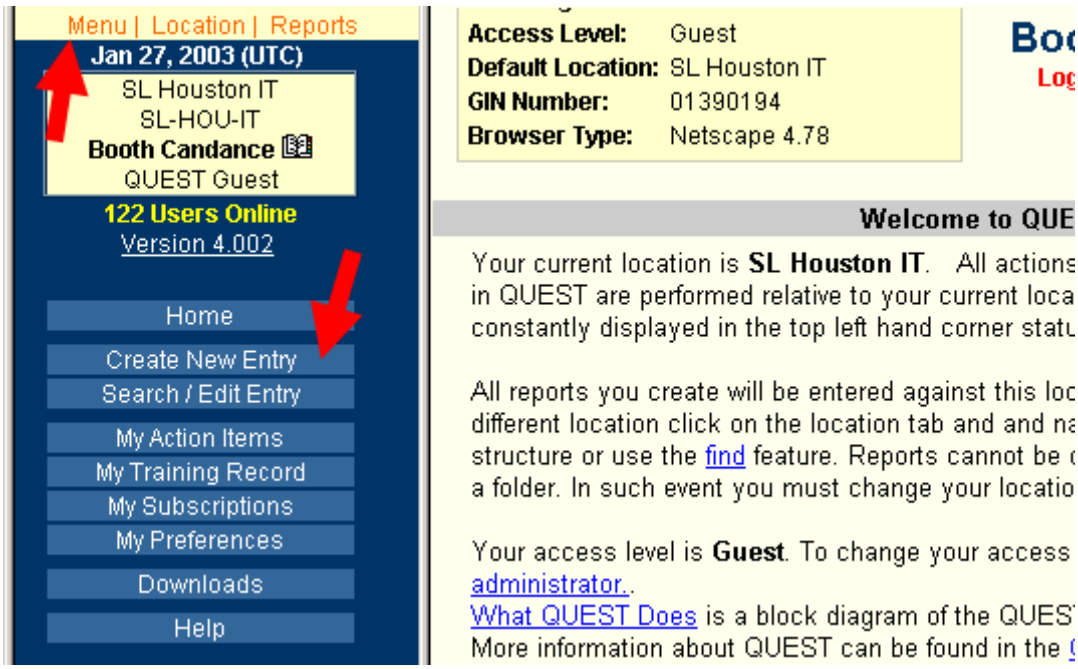
CLASIFICACIÓN	INFORMACIÓN	MEDIDAS DE SEGURIDAD APROPIADAS
	de nuevo personal y de Mercadeo	

Figura 2-14: Clasificación de la información en Omnes

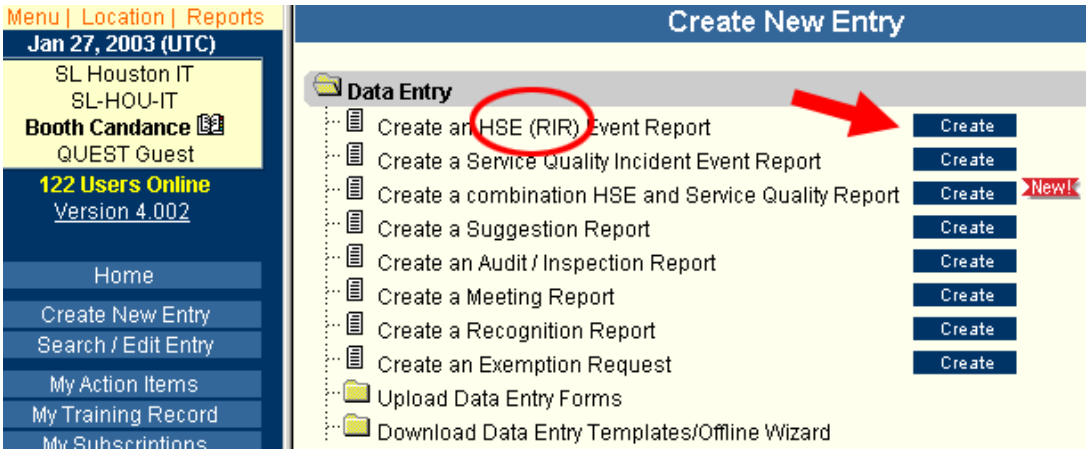
2.7. PROCEDIMIENTOS EN REPORTAR E IDENTIFICAR RIESGOS

Los incidentes reales o potenciales son reportados usando la herramienta de reportes de riesgos denominada QUEST. El siguiente procedimiento resume las opciones relacionadas directamente a los incidentes en seguridad de información.

1. Abra una ventana del navegador Internet Explorer. Debido a que algunas opciones de la página no funcionan bajo el navegador de Netscape.
2. Vaya a la dirección de QUEST. http://quest.slb.com /
3. Si es necesario, ajusta su situación, usando el enlace del menú locación en la parte superior derecha de la ventana.
4. Bajo el menú Principal, haga clic en el botón Create New Entry.

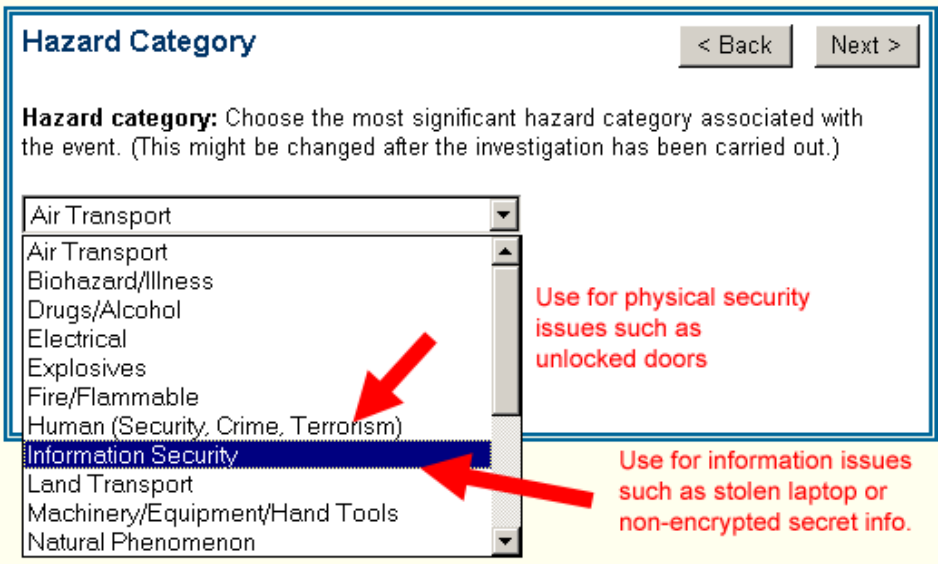


5. En la siguiente opción "Create an HSE (RIR) Event Report," haga clic en el botón Create..



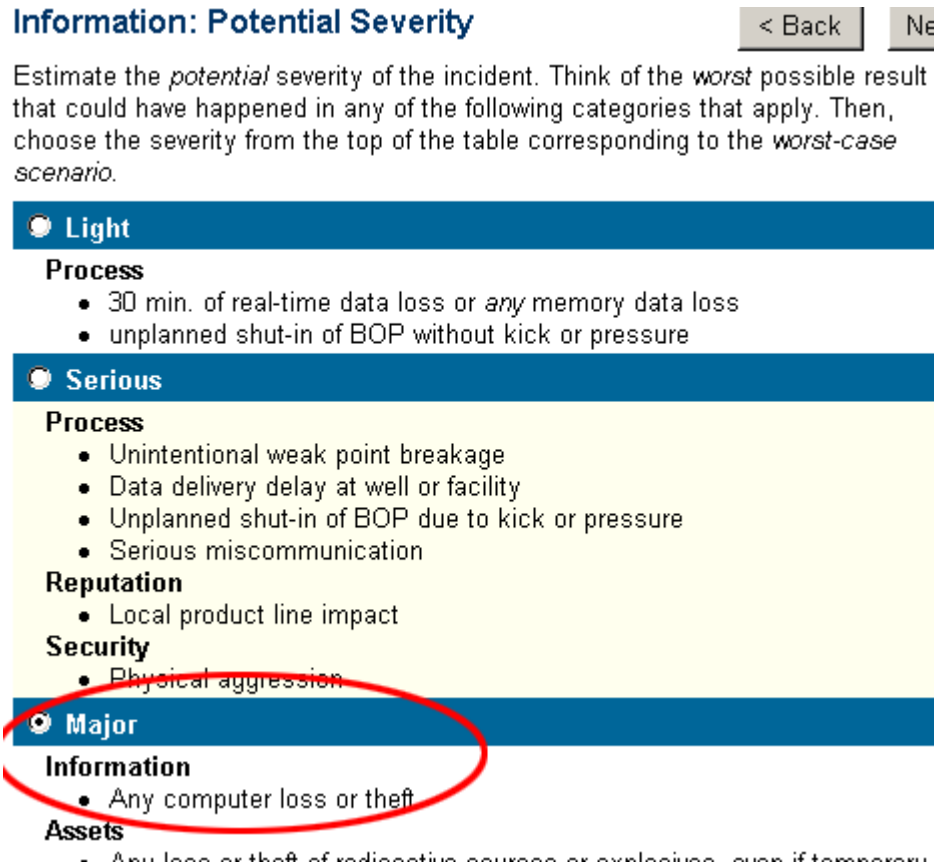
6. Seleccione el enlace al tipo de reporte que desea crear. Nosotros le recomendamos seleccionar Crear un Evento con el Asistente, el cual explica cada opción del informe.

7. Cuando tenga en pantalla la ventana inicial de la herramienta teclee "Hazard Category," seleccione Seguridad de la Información para incidentes potenciales o actuales que involucran datos. Un problema de acceso al edificio podría listarse en cambio como humano.



8. A continuación aparecerá una pantalla de "Severidad Potencial," poniendo como ejemplo el robo de una computadora seleccionaríamos la opción de

mayor de acuerdo a nuestro caso. El Asistente le explicará lo que se significa cada una de las opciones que le presenta Ligth, Serious, Mayor, y Catastrophic.



9. Usted no necesita realizar ninguna otra acción. Esto será completado por su SSO u otros administradores notificados por el sistema.
10. Si usted taso esta casualidad como catastrófico, mayor, o serio, avise a su SSO además de rellenar este informe del QUEST

2.8. LEVANTAMIENTO DE ÁREAS FUNCIONALES

Entiéndase por áreas funcionales los departamentos que conforman la estructura organizacional de la compañía, que tiene funciones o actividades independientes y diferentes que promueven el desarrollo de la compañía y la competitividad de la misma.

2.9. ORGANIGRAMA ESTRUCTURAL DE OMNES

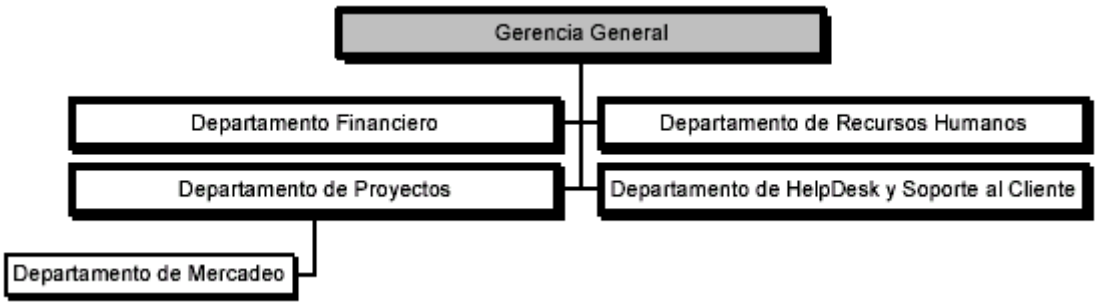


Figura 2-15 Organigrama funcional de Omnes

2.10. ORGANIGRAMA FUNCIONAL DE OMNES

DEPENDENCIA	FUNCION
Gerencial	Manejo y Dirección de la compañía. Toma de Decisiones. Relacionarse internacionalmente con otras compañías.
Financiero	Operaciones Financieras. Manejo de Procesos Contables y asignación de presupuestos. Manejo de Recursos Económicos de la compañía. Facturación a los clientes. Manejo legal de la parte Financiera.
Recursos Humanos	Planificación de los objetivos del empleado. Análisis de los objetivos de los empleados anualmente Recepción de quejas y sugerencias hacia la empresa. Coordinación de actividades y eventos sociales.
HelpDesk y Soporte al Cliente	Operación y Control de Tecnología de la Información. Coordinación y todo lo que respecta a tecnología de la informática a los clientes.

DEPENDENCIA	FUNCION
	Operación del área de Sistemas y Telecomunicaciones. Soporte al cliente en lo que respecta a informática y telecomunicaciones. Administración general de la red de información. Realización de respaldos de la información Coordinación de la seguridad de la información Control de acceso físico a las instalaciones.
Proyectos	Manejo y ejecución de nuevos Proyectos. Dirección de proyectos en marcha. Coordinación de nuevas propuestas para los clientes. Análisis de necesidades de los clientes.
Mercadeo	Establecimiento de Alianzas Estratégicas. Captación de nuevos clientes. Ventas de servicios Ventas de productos.

Tabla 2-16 Areas funcionales de la Compañía.

2.11. LEVANTAMIENTO DE INFORMACIÓN DE RECURSOS HUMANOS

A continuación se describe los cargos, con su perfil, sus funciones, y sus actividades dentro de lo cual la compañía a contratado su personal para la realización de sus actividades, y el cumplimiento de los objetivos de la compañía.

Gerente General

Titulo del Cargo: Gerente para la Zona Andina

Propósito del Cargo: Coordinar el desarrollo de las operaciones en los países andinos para obtener los resultados y metas establecidas para la zona: Colombia, Ecuador, y Perú.

Principales Deberes y Responsabilidades:

- Llevar el control administrativo y financiero de los proyectos (smart cards, outsourcing, cableado estructurado,) realizados en el país.
- Hacer un seguimiento del desempeño del personal del país.
- Visitar las diferentes Oficinas de los clientes para lograr mayor control de las operaciones.
- Actuar como enlace entre Ecuador, Colombia y Perú (suministrar información relacionada en lo económico y de la situación de competitividad de la empresa en el país).
- Captar nuevos clientes y negocios.
- Mercadeo en la zona.

Información general del Cargo

Tiene 4 empleados bajo su supervisión directa y 35 bajo supervisión indirecta.

Es responsable por presupuesto de gastos, presupuesto de inversiones y volúmenes de ventas.

Maneja información estratégica y técnica del cliente (confidencial).

Conoce la información salarial de sus empleados y de Recursos Humanos.

Se relaciona continuamente con los Presidentes y Gerentes Generales de las empresas, con el Gerente Regional y con los proveedores más importantes; las reuniones con los Gerentes de otras regiones son ocasionales.

Toma decisiones relacionadas con márgenes de venta, niveles técnicos, alcance de servicio, que son previamente revisadas y aprobadas por el Gerente Regional.

Las dificultades que presenta el cargo tienen que ver con la coordinación de logística y recursos en diferentes localidades y el logro del apoyo necesario en cada país.

Nivel Académico y Técnico: Nivel Universitario, preferiblemente Ingeniería Electrónica; deseable: Post-Grado en negocio y ventas.

Conocimientos Técnicos Especiales, Destrezas o Aptitudes

Ventas.

Técnicas de manejo de personal y supervisión.

Ingles

Experiencia

Mínimo 10 años de experiencia en cargos gerenciales similares.

Ventas.

Manejo de Personal

Habilidades y Actitudes Requeridas

Manejo de relaciones interpersonales.

Habilidad numérica.

Capacidad de dirigir y asignar responsabilidades.

Capacidad de integración.

Capacidad de generar motivación.

Capacidad de influir sobre otros.

Capacidad para convencer y generar confianza.

Características Adicionales

Disponibilidad para viajar frecuentemente.

Dinámico.

Flexible

Capacidad de adaptación

Asistente Administrativo

Titulo del Cargo: Asistente Administrativo.

Propósito del Cargo: Manejo administrativo de las operaciones (Pago de impuestos, Pago a los empleados, y Cobro a los clientes) y coordinación de actividades en un tiempo prudencial y de acuerdo a los requerimientos y prioridades.

Principales Deberes y Responsabilidades:

- Reporte de ingresos y facturación de outsourcing, cableado estructurado y smart cards.
- Reporte de gastos y caja chica.
- Logística general: Trámite de visas, Coordinación de viajes y demás servicios generales.
- Responder las solicitudes de los empleados.(Retroactivos, Sueldos, Vacaciones, Cursos de especialización)
- Correspondencia interna y externa, cartas de trabajo.
- Compras y trámites aduaneros.
- Coordinar citas con clientes, visitas internas y en el exterior.

Información General del Cargo:

No tiene personal bajo su supervisión.

Es responsable por la adquisión de computadores, fax Modem, tarjetas de red, cables.

Tiene acceso a información confidencial de tipo contable: costos fijos de la Región andina, márgenes de ganancia y conoce aspectos relacionados con la compensación de los empleados, bonos asignados eventualmente a cada uno.

Se relaciona todo nivel, con clientes, proveedores, agentes aduaneros, empleados y gerentes de la misma compañía en otros países.

Toma decisiones de rutina, relacionadas con la logística interna y propone soluciones a los problemas que se presentan; sus decisiones no tienen gran impacto sobre los compromisos que adquiere la empresa y son revisadas por su supervisor.

Las dificultades que presenta el cargo tienen que ver con la coordinación de viajes y actividades de los empleados que trabajan fuera de la oficina (en el campo o en ciertos proyectos).

Nivel Académico y Técnico: Nivel Técnico con especialidad en Contabilidad.

Conocimientos Técnicos Especiales, Destrezas o Aptitudes

Manejo de Ingles.

Manejo de programas de computación (Word, Excel, Power Point).

Experiencia

1 año de experiencia en trabajo de Oficina.

Coordinación de actividades.

Habilidades y Actitudes Requeridas

Planificación y coordinación de actividades.

Buenas relaciones interpersonales.

Facilidades de comunicación.

Capacidad de adaptación y de afrontar cambios.

Proactividad.

Iniciativa.

Características Adicionales

Buena presencia

Personalidad abierta.

Persona Organizada.

Buena memoria.

Detallista.

Rapidez.

Soporte LAN / WAN

Titulo del Cargo: Soporte LAN/WAN

Propósito del Cargo: Dar soporte a las redes LAN/WAN de los clientes, tanto en el campo como en la ciudad.

Principales Deberes y Responsabilidades:

- Instalación y configuración de Inmarsat (configuración correo de voz, puerto de fax y puerto de datos de media y alta velocidad).

- Transmisión de archivos de registros.
- Troubleshooting y configuración de sistemas WAN basados en Cisco.
- Soporte de sistemas basados en Windows.
- Actualización de LDAP (Registro electrónico único del empleado).
- Troubleshooting en problemas de conectividad.
- Diseño e instalación de sistemas de cableado estructurado basados en UTP-5 y en fibra óptica.

Información General del Cargo

No tiene personal bajo su supervisión.

Es responsable por los equipos que instala y configura.

Conoce las características de la red de los clientes y maneja información confidencial de los mismos.

Sus relaciones van desde niveles técnicos, con usuarios hasta gerentes y clientes.

Toma decisiones referentes a la instalación y configuración de los equipos que conforman el sistema; de sus decisiones depende la versatilidad, capacidad y buen funcionamiento del sistema; estas decisiones son supervisadas por el gerente de la Zona Andina.

Requiere actualización de sus conocimientos.

Calificaciones Académicas y Técnicas: Nivel universitario con especialidad en Ingeniería Electrónica; deseable: Post-Grado en Telecomunicaciones o Maestría en Ciencias Electrónicas.

Conocimientos Técnicos Especiales, Destrezas o Aptitudes

Dominio del Inglés técnico y conversacional.

Configuración de Routers Cisco.

Diseño de redes.

Windows (NT, 95, 98, 2000).

Sistema Unix.

Cableado estructurado.

Sistema de comunicación.

Experiencia.

Area de comunicaciones.

Area de Sistemas.

Area de Conectividad.

Habilidades y Actitudes Requeridas

Habilidad numérica.

Facilidad de comunicación.

Capacidad de Adaptación.

Capacidad para trabajar bajo presión.

Paciencia.

Características Adicionales

Buen estado físico y alta disponibilidad para viajar al campo (Selva).

Preferiblemente Soltero.

Resistencia Física.

Condiciones de trabajo difíciles (Selva).

Soporte HelpDesk

Titulo del Cargo: Soporte HelpDesk

Propósito del Cargo: Canalizar las solicitudes de soporte técnico de los usuarios.

Principales Deberes y Responsabilidades:

- Atender la llamada y registrar la solicitud.
- Ingresar un ticket a una base de datos donde se coordina su atención de acuerdo a las prioridades.
- Si desde el HelpDesk se puede solucionar el problema se cierra el ticket en caso contrario, se asignará dicho ticket a la persona adecuada.
- Realizar el seguimiento del ticket para garantizar la atención en un tiempo óptimo.

Información General del Cargo

No tiene personal bajo su supervisión.

Es responsable por computadoras, impresoras, hardware.

Tiene acceso a las cuentas de e-mail de los usuarios.

Se relaciona con el usuario a todo nivel.

Sus decisiones tienen que ver con la resolución de los problemas técnicos que se le presentan a los usuarios; son revisadas y aprobadas por el Gerente de Proyecto.

Presenta dificultades por la cantidad de llamadas recibidas en ciertas horas, disponibilidad de herramientas y lugar de trabajo, caluroso y muy pequeño.

Calificaciones Académicas y Técnicas: Ingeniería de Sistemas, Electrónica o nivel técnico con experiencia equivalente.

Conocimientos Técnicos Especiales, Destrezas o Aptitudes

Hardware.

Software, Aplicaciones.

Sistemas operativos.

Correo electrónico.

Ingles técnico y conversacional.

Experiencia

Tres años de experiencia en atención a usuarios.

Sistemas operativos, paquetes de software y hardware.

Habilidades y Actitudes Requeridas

Facilidad para comunicarse y expresarse.

Capacidad de resolver problemas con rapidez.

Capacidad para trabajar bajo presión.

Paciencia.

Pensamiento lógico y sistemático.

Facilidad explicativa.

Características Adicionales

Interés por aprender (autoentrenamiento, investigación).

Dinamismo.

Ser cortes y educado.

Voz agradable.

Gerente de Proyecto

Titulo del Cargo: Gerente de Proyecto

Propósito del cargo: Gerenciar el negocio de Omnes en Ecuador mediante el control de las Operaciones, ventas y administración.

Principales Deberes y Responsabilidades

Buscar nuevos negocios desarrollando estrategias de venta y mercadeo.

Preparar las propuestas técnicas y económicas que satisfagan los requerimientos de los clientes.

Manejo y/o supervisión de los proyectos para lograr los objetivos técnicos y económicos ofertados.

Supervisión de las actividades técnicas y operativas.

Supervisión de las actividades administrativas y financieras.

Manejo de personal.

Información General del Cargo

El Project Manager tiene bajo su supervisión 6 empleados; 4 bajo supervisión directa y 2 indirectamente.

Es responsable en forma directa por presupuesto de gastos y volúmenes de ventas, y en forma indirecta por presupuesto de inversiones.

Tiene acceso a información confidencial de mediano y alto impacto relativa a los clientes, planes de negocio, información administrativa y financiera, e información de Recursos Humanos.

Toma decisiones referentes a nuevos negocios y pérdida de oportunidades, aumento de costos directos e indirectos, nuevas inversiones y contratación de personal; todo lo relacionado con aumento de costos indirectos, contratación de personal y nuevas inversiones, es consultado.

Presenta ciertas dificultades: captación de nuevos negocios, relación con el cliente, logro de los resultados del Budget (Revenue/Neto), manejo del personal y de las operaciones, y desarrollo de procedimientos operativos y administrativos.

Calificaciones Académicas y Técnicas: Nivel universitario con especialidad en informática o electrónica; deseable: Postgrado en Gerencia de Proyectos.

Conocimientos Técnicos Especiales, Destreza o Aptitudes

Dominio del Ingles.

Cursos de Administración de Empresas.

Nuevas Tecnologías que aparecen en el mercado para conocer lo que se vende.

Contabilidad y Finanzas a nivel básico.

Experiencia

Cinco años de experiencia en ventas, gerencia de sistemas o de proyectos, área de sistemas, manejo de personal, contabilidad y finanzas.

Habilidad y Actitudes Requeridas

Visión de negocios

Habilidad para negociar.

Capacidad de dirigir y asignar responsabilidades.

Capacidad para supervisar personal.

Capacidad para trabajar bajo presión y fuera de horario fijo.

Facilidad para dar soluciones o salidas a problemas.

Características Adicionales

Persona organizada

Buena memoria.

Proactividad.

Trabajo en equipo.

Liderazgo.

Ejecutivo de Ventas

Titulo del Cargo: Ejecutivo de Ventas

Propósito del Cargo: Lograr mayor penetración en el mercado informático y posicionar a Omnes como empresa de servicios de Telecomunicaciones.

Principales Deberes y Responsabilidades

- Promover la venta de proyectos y nuevos negocios.
- Atender a los clientes, realizar visitas.
- Ganar nuevos clientes.

- Buscar información de los clientes de Omnes y contactar a los clientes potenciales para servicios de Telecomunicaciones, Seguridad (SmartCards) y Outsourcing

Información General del Cargo

No tiene personal bajo su supervisión.

Maneja información confidencial relativa a cotizaciones y costos.

Se relaciona con su supervisor, clientes,, posibles clientes y mayoristas.

Toma decisiones que tienen que ver con contratos de servicio y órdenes de compra.

Las dificultades que presenta el cargo se basan en el mercadeo de la empresa en Ecuador: falta de eventos para promocionar los servicios de la compañía (Workshops); carencia de publicidad en medios especializados locales; definición de funciones de equipos técnicos; inexistencia de estrategias para lanzar nuevos productos.

Requiere conocimiento de productos y servicios a ofertar.

Calificaciones Académicas y Técnicas: Nivel universitario preferiblemente con estudios en Ingeniería; deseable: post-grado o estudios de mercadeo o negocios.

Conocimientos Técnicos Especiales, Destrezas o Aptitudes

Manejo de los productos y servicio que ofrece la compañía.

Dominio del Idioma Ingles.

Técnicas de Venta.

Experiencia

Haber trabajando en desarrollo y manejo de proyectos.

Habilidad y Actitudes requeridas

Facilidad de comunicación explicativa.

Habilidad para convencer e influir sobre otras personas.

Capacidad de negociación.

Visión de negocios.

Características Adicionales.

Persona abierta y dinámica.

Buena memoria.

Rapidez mental.

2.12. LEVANTAMIENTO DE ORGANIZACIÓN DEL CENTRO DE CÓMPUTO.

El llamado “Cuarto de Servidores” alberga al Servidor de Correo Electrónico, Domain Name Server y Aplicaciones (NT) y al Servidor de Información y DHCP (NT-B). Además, alberga una estación utilizada con la Base de Datos Oracle 8.1 para desarrollo de aplicaciones de Tarjetas Inteligentes y otra estación con Windows 95 la cual maneja el software de Control de Accesos y Alarmas (Keri Systems) y el consumo telefónico emitido por la Central Telefónica.

EQUIPOS DE COMUNICACIÓN	CANTIDAD
Router CISCO	2
HUB 3COM	7
SWITCH 3COM	1
Cache Flow	1
Central Telefónica ALCATEL 4400	1

Tabla 2.17 (Equipos de Comunicación).

Acceso Físico al Cuarto de Servidores: Para el acceso al Cuarto de Servidores se dispone de una cerradura electrónica con clave, la misma que es conocida por todo el personal del Departamento de HelpDesk.

Sistema de enfriamiento para Cuarto de Servidores: El Cuarto de Servidores si cuenta con un sistema de aire acondicionado exclusivo para el enfriamiento de los equipos.

Seguridades del Cuarto de Servidores: Con excepción de la cerradura electrónica para acceso al cuarto, el mismo no dispone de otras protecciones, cajas fuertes u otros implementos para salvaguarda de la información.

Central Telefónica: La Central Telefónica marca ALCATEL se encuentra ubicada en el Cuarto de Servidores, la misma dispone de cuatro baterías externas para casos de emergencia.

Adicionalmente a las baterías que dispone, la Central Telefónica se encuentra al momento conectada a un UPS individual, el cual proporciona 30 minutos de energía.

2.13. LEVANTAMIENTO DE INFORMACIÓN FÍSICO Y LÓGICO DE LA RED.

Con respecto a la red Lan (Red de Area Local), la compañía dispone de un completo sistema de cableado categoría 5 en todo en todo lo que comprende el piso donde realiza sus operaciones, con dos puntos de red por usuario (cubículo), con velocidades de transmisión e hasta 100 Mega bits por segundo. Ver diagrama de distribución física sección Anexos (Anexo 2) En el piso se dispone de dos Hubs Ethernet 3COM de 10/100 Mbps cada uno, cada toma cumple con las normas de categoría 5 UTP.

La red WAN (Red de Área Extendida), se extiende por casi 80 países en el mundo entero. En el Ecuador la Intranet de Omnes, llamada SINET, conecta a las ciudades de Nueva Loja y Quito, con la posibilidad de extenderse hasta Guayaquil en el próximo año. La mayoría de usuarios tienen acceso a comunicación por medio de RAS (Remote Access Server) a través de cuentas Dial-Up para

conexión telefónica para lo que es Internet y Correo Electrónico. Se maneja el protocolo TCP/IP y la red Windows NT.

La salida a Internet se la hace a través de un dispositivo llamado Cache Flow, el cual permite que el flujo de información referente a Internet entre y salga a través de un proveedor local (ISP) y lo que se refiere a Intranet a través de un enlace exclusivo hacia Houston. Está por implementarse una Red Privada Virtual (VPN) en lo que a Ecuador se refiere, pues en otros países donde la compañía opera ya existe esta tecnología a través de proveedores de Internet. Adicionalmente, la compañía cuenta con una moderna Central Telefónica ALCATEL modelo 4400, la cual permite tener acceso a una serie de servicios tales como: correo de voz, funciones de forward, anuncio de mensajes e itinerarios, servicio de directorio, entre otros. Actualmente la Central brinda acceso a 183 empleados en Quito y con posibilidad de aumentarse a los 200 en los próximos meses.

Hardware

A continuación se detallan los equipos de computación existentes en la compañía con su respectivo modelo. Cabe indicar que todos los equipos son marca DELL por estándar de Omnes a nivel mundial.

Adicionalmente, se detallan las impresoras existentes con su respectiva marca y modelo.

Modelo de Computador	Cantidad
Dell Optiplex GX110 (Desktop)	5
Dell Optiplex GX150 (Desktop)	6
Apple IMAC G3	4
Dell Latitude LS (Laptop)	3
Dell Latitude C600 (Laptop)	5
Compaq Armada 1500 (Laptop)	1
Dell Optiplex GX1 (Desktop)	1

Tabla 2-18: Modelo de Computador

Modelo de Impresora	Cantidad
HP Deskjet 820 Cxi	1
HP 1100 (Láser)	1
HP Deskjet 920C	1
HP 4100 (Láser)	1

Tabla 2-19: Modelo de Impresoras

2.14. LEVANTAMIENTO DE INFORMACIÓN DE PROCESOS

A continuación se detallarán todos los procesos que se realizan en todas las áreas de la compañía de forma detallada conforme a lo contestado en el cuestionario realizado (Anexo 1)

2.14.1. Administración de Servidores

Este proceso lo realiza una persona se encarga de verificar que todos los servicios se encuentre subidos en cada uno de los servidores se encarga también de verificar que haya espacio disponible en los discos, que las tasas de consumo de recursos de hardware (memoria y procesador) no sea alta y si lo es se encarga de eliminar otros procesos que no tengan mayor importancia como desconectar usuarios, tiene mayor carga de trabajo toda la semana laborable, es decir de Lunes a Viernes, y los días cuando se realiza actualización de servidores, tiene el grado de catastrófico si el proceso que se realizan en estos equipos llegase a detenerse, perjudicaría a la organización, el tiempo que puede pasar detenido es de 12 horas laborables, el tiempo que se demora en restablecerse es de 2 horas, no existen documentos o instructivos para desarrollar el proceso.

Actividades que desarrollan para la ejecución del proceso:

Control de servidores caídas, problemas

Instalación de Aplicaciones en los servidores

Verificación de espacio en disco en cada servidor.

Verificación de cuentas de e-mail y de red

Administración de derechos sobre fólder y archivos

Backup de servidores.

Para el respaldo de la información existe un cronograma predeterminado, es decir, existen políticas para respaldar la información crítica con un horario programado, para el respaldo de datos será la unidad Super DLT con que consta el servidor Connected1-ecu. El dispositivo sobre el que se ejecutará el backup es: Media Set. El responsable de la selección de los datos a respaldar y la generación de los trabajos en el Backup Exec “Sistema de respaldo de Datos” es: Santiago Jaramillo. Los responsables de los cambios de cintas serán: Mario Recalde y Wilson Suárez. Los responsables de la recuperación de datos serán: Help Desk.

DIA	HORA	SERVIDOR	TIPO DE BACKUP
Martes	6:00	nt-b	Incremental
	4:00	nt/nt-monitor	Incremental
Miércoles	6:00	nt-b	Incremental
	4:00	nt/nt-monitor	Incremental
Jueves	6:00	nt-b	Incremental
	4:00	nt/nt-monitor	Incremental
Viernes	19:00	nt/nt-monitor	Total
	20:00	nt-b	Total

Tabla 2-20: Frecuencia de respaldos de la información.

2.14.2. On site Support

Este proceso lo realizan cuatro personas del departamento de helpdesk cada uno de ellos se encarga de dar soporte técnico vía telefónica al usuario “Cliente” cuando tiene problemas en el manejo de alguna aplicación, el proceso tiene carga de trabajo la mayor parte de la semana laborable desde los días Lunes a Jueves, cuando los usuarios no están informados de cambios realizados por el personal

de Helpdesk y cuando los usuarios no se encuentran suficientemente entrenados en el uso de aplicaciones técnicas y necesitan asistencia del personal de Soporte técnico, el grado de perjuicio hacia la empresa es de moderado, si el proceso llegase a interrumpirse, el tiempo que puede pasar sin darse asistencia técnica a los usuarios es de 4 días laborables, el tiempo tolerable en restablecerse el soporte técnico es de 2 horas, existen pocos documentos o instructivos para desarrollar el proceso, estos pertenecen a aplicaciones que la empresa desarrolladora del software otorga a Omnes como parte del servicio al cliente, en lo que respecta a soporte técnico de ingreso a la red no existe ningún documento.

Actividades que desarrollan para la ejecución del proceso:

Dar soporte a los usuarios en los problemas que tengan en su PC o en la red.

2.14.3. Ventas con Clientes Externos

Este proceso tiene mayor carga de trabajo en los días previos que tenga que realizarse envíos de presupuestos a clientes por la realización de un determinado proyecto, tiene el grado de menor si el proceso llegara a obstruirse o detenerse generalmente ocurriría esto por la falta de conocimientos de precios en materiales, y que la compañía no contiene en stock y demandaría importar e implicaría gastos lo que le dificultaría la realización de un presupuesto adecuado y real, el tiempo que puede retrasarse o pasar detenido es de 1 mes laborable, el tiempo que le toma en restablecerse es de un mes, no existen documentos o instructivos para desarrollar el proceso, pues generalmente los procedimientos varían de acuerdo los trámites burocráticos al que la compañía tiene que sujetarse.

Actividades que desarrollan para la ejecución del proceso:

Promoción de servicios

Contactarse con los clientes potenciales.

Elaboración de presupuestos.

2.14.4. Administración del sistema de seguridad y Soporte técnico a Ventas.

Este proceso lo realiza una persona que se encarga del mantenimiento del sistema Keri System las operaciones que realiza esta persona es de mantener operativo al sistema las 24 horas del día además colabora con el departamento de ventas en la parte técnica, el proceso tiene mayor carga de trabajo los días Lunes, Martes y Viernes, tiene el grado de moderado si el proceso llegase a detenerse, esto puede ocurrir cuando el sistema se cae, esto se debe a que el sistema no es fiable y se produce por mayor afluencia de personas que ingresan y salen del edificio y el sistema de monitoreo no soporta el controlar todos los pisos del edificio, en lo que respecta en el soporte técnico a Ventas la persona encargada de la administración del sistema de seguridad debe coayudar en el desarrollo de proyectos de seguridad de instalaciones mediante smart cards su ausencia es tolerable y superable, el tiempo que puede pasar detenido es de dos días, no existen documentos o instructivos que orienten en el desarrollo del proceso.

Actividades que se desarrollan para la ejecución del proceso:

Monitorear y configurar el sistema de acceso

Ayudar en la realización de propuestas económicas

Participar en el proyecto y su implementación

2.14.5. Administración de Proyectos

Es la captación de clientes potenciales para lo cual el jefe del departamento de proyectos prepara estrategias de mercadeo, este proceso tiene mayor carga de trabajo toda la semana laborable, tiene el grado de moderado si el proceso llegara a detenerse, el tiempo que puede pasar detenido es de un mes laborable, el tiempo que se demora en restablecerse es de un mes, no existen documentos o instructivos para desarrollar el proceso.

Actividades que desarrollan para la ejecución del proceso:

Promoción de servicios

Contactarse con los clientes potenciales.

Elaboración de presupuestos.

2.14.6. Coordinación de los Servicios.

El proceso lo realiza una persona que se encarga de controlar que todas las inquietudes o necesidades de los clientes hayan sido resueltas, este proceso tiene mayor carga de trabajo toda la semana laborable, tiene el grado de moderado si el proceso llegara a detenerse, el tiempo que puede pasar detenido es de un día laborable, el tiempo que se demora en restablecerse es de un día como máximo, no existen documentos o instructivos que oriente en el desarrollo del proceso.

Actividades que desarrollan para la ejecución del proceso:

Coordinación de las necesidades actuales y futuras de los clientes.

Coordinación del servicio prestado a los clientes

Análisis del presupuesto del cliente

Control de calidad del servicio prestado al cliente.

Control del personal de sistemas y telecomunicaciones de la compañía.

2.14.7. Coordinación de Recursos Humanos.

Este proceso es muy simple lo realiza una persona que es la secretaria de Gerencia, que se encarga de organizar eventos sociales y de transmitir inquietudes al departamento de Recursos Humanos, este proceso tiene mayor carga de trabajo es en días previos de un evento o días especiales, tiene el grado

de menor si el proceso llegara a detenerse, el tiempo que puede pasar detenido es de una semana, el tiempo que se demora en restablecerse es de una semana, no existen documentos o instructivos que orienten el desarrollo del proceso.

Actividades que desarrollan para la ejecución del proceso:

Servir de nexo entre el personal de Omnes y RRHH

Coordinación de actividades y eventos especiales para el departamento de ventas. Coordinación de eventos especiales para el personal de Omnes.

Servir de Secretaria de Gerencia.

2.14.8. Manejo del área de contabilidad de la compañía.

Es el manejo del área de contabilidad, de determinar ingresos y egresos de llevar presupuestos, y de pagar sueldos a los trabajadores, y de informar a Omnes Colombia sobre la situación financiera de la Compañía en Ecuador, este proceso tiene carga de trabajo la última semana del mes y del año por cierre del libro, tiene el grado de moderado si el proceso llegara a detenerse, el tiempo que puede pasar detenido es de una semana laborable, el tiempo que se demora en restablecerse es de dos días que es en el peor de los casos, no existen documentos o instructivos que orienten en el desarrollo del proceso.

Actividades que desarrollan para la ejecución del proceso:

Manejo de nomina

Roles de pago.

Manejo de caja chica.

Control del personal financiero bajo su supervisión

Revisar el estado financiero de la compañía.

Toma de decisiones de orden financiero de la compañía.

2.14.9. Accesos Físicos a las instalaciones

Es la vigilancia que se cumple dentro y fuera del edificio, para lo cual se cuenta con guardianía privada, la cual controla las 24 horas el acceso al edificio por su entrada principal, lamentablemente no se sigue un control riguroso de las personas que ingresan al mismo en el sentido que los guardias no cuentan con detector de metales, la compañía Omnes se encuentra ubicada en el quinto piso del edifico Siglo XXI en donde operan el resto de compañías que integran el grupo Schlumberger del Ecuador, para el ingreso al edificio cada trabajador debe portar su smart card personal que debe ser leído por cada lector de tarjetas que se encuentran ubicados en cada puerta de ingreso a un piso del edificio el cual lo habilitara o no dependiendo de su lugar de trabajo y horario de trabajo, como se menciono anteriormente el sistema que controla el acceso denominado KERI SYSTEMS no es muy fiable cuando existe demasiada afluencia de personas que ingresan o salgan del edificio, es decir cuando existen horas picos, para personas ajenas a Schlumberger deben presentar su cédula de identidad para que puedan ingresar y se les otorga una tarjeta con el número del piso donde van a realizar su diligencia, es válida únicamente para ese piso el ingreso de cada persona es monitoreado y almacenado en un base de datos en SQL SERVER, el sistema es el KERI SYSTEMS, el cual almacena el nombre de la persona, la hora que ingresa y la hora que sale y a que número de piso ingresa, en cuanto el ingreso al departamento de helpdesk es restringido existía un sistema de ingreso por huella digital y clave personal el cual presentaba falencias durante el tiempo que paso operando, actualmente no existe ningún sistema de protección de ingreso al departamento de helpdesk, el ingreso al cuarto de servidores cuenta con un sistema de clave el cual la conocen tres personas encargadas de la administración del lugar el sistema es fiable y no a producido falencia alguna.

III.- POLITICAS Y PROCESOS DE SEGURIDAD

3.1. INTRODUCCIÓN

El conjunto de políticas de seguridad de información definen las medidas requeridas para proteger los recursos de información mientras se da cumplimiento con los requisitos comerciales y otras obligaciones para la protección de la información.

Estas políticas y procesos describen las responsabilidades en seguridad de información de cada usuario de información de Omnes y sistemas (medios informáticos). La política debe incrementar el conocimiento del usuario en precauciones en seguridad de la información de lo cual se espera que los usuarios las tomen para apoyar la seguridad de información corporativa. El propósito es reducir el riesgo de daño, robo, fraude, abuso o mal uso de los medios informáticos. Estas políticas se aplican al usuario empleado y al usuario no empleado que hacen uso de los sistemas e información de Omnes.

3.2. POLÍTICAS PARA LOS REGISTROS VITALES

Los empleados, consultores, o contratistas que trabajan dentro de los medios de Omnes o por estar conectado a su red o tener acceso remoto obedecerán las condiciones de esta política. La falta de cumplimiento puede resultar en la pérdida inmediata de todos los privilegios de acceso. El uso de cualquier recurso de Omnes de una manera impropia o poco profesional es inaceptable y producirá acción disciplinaria que puede incluir la terminación de las relaciones laborales con dicha persona o empresa. El Incumplimiento será reportado usando la herramienta de reportes de identificación de riesgos corporativa (QUEST).

3.2.1. Proceso de clasificación de Información

El esquema de la clasificación se aplicará a la información impresa (papel); los archivos electrónicos que se guardaron en medios de comunicación trasladables (CD-ROMs, las cintas, los disquetes flexibles); discos duros de equipos de oficina o portátiles o equipo de comunicación; los datos que se transmitieron usando medios electrónicos. Los siguientes párrafos describen las categorías de clasificación de seguridad a ser aplicadas en Omnes sobre los Recursos de

información. Los requisitos para etiquetar, guardar, disponer de, o alguna otra manera de manejar recursos clasificados se describen en el Proceso de clasificación de los registros vitales.

a) Lo Secreto de Omnes – La Información que proporciona la organización con un grado de competitividad significante, que muestra estrategias comerciales específicas y directrices organizacionales, lo que es esencial para el éxito técnico o financiero de un producto específico o servicio es clasificado como secreta. El descubrimiento desautorizado de este tipo de información causaría un daño serio a los intereses de la compañía. La severidad de un incidente de seguridad de información que involucra el acceso desautorizado a la información secreta se informará como Catastrófico o Multicatastrófico, dependiendo de la información del impacto financiero o tiempo a recuperase. Los ejemplos de información secreta incluyen:

- La información de una significante adquisición o proyecto de Inversión.
- Información que podría afectar el precio de las acciones
- Información que tiene la sensibilidad política, financiera, o legal.
- Información de sobre una reorganización mayor o eso tiene un impacto en Recursos Humanos.

b) Lo confidencial de Omnes. Se aplica a la información que, si se descubriera, sería perjudicial a los intereses de la compañía o causaría un daño serio al interés de la compañía o a sus empleados. Una casualidad de seguridad que involucra el acceso desautorizado a la información Confidencial tendrá un nivel de severidad de Catastrófico, dependiendo de la información del impacto financiero o tiempo a recuperase. Lo siguiente son los recursos como ejemplos de información Confidencial:

- Contratos
- Los datos de los clientes.
- La información técnica que afecta la ventaja competitiva de la compañía
- La información personal o personal relacionada (por ejemplo el sueldo, evaluaciones del desempeño de un trabajador).

c) Lo privado de Omnes. Se aplica a la información disponible para los empleados de la compañía y autorización a terceras personas (por ejemplo contratistas, internos, etc.) como parte de un negocio de rutina. Una casualidad en seguridad que involucra el acceso desautorizado a la información privada de Omnes tendrá un nivel de severidad de Serio o Mayor, dependiendo en adelante del impacto financiero o del tiempo a recuperase, pero nunca menos serio. Los recursos de información no etiquetados son considerados como Privada por defecto. Los siguientes son los recursos como ejemplos de información privada:

- El correo electrónico interno de la Compañía
- Los datos del Directorio Corporativo

d) Lo Público de Omnes Se Aplica a la información que la compañía o de manera individual hace disponible a los clientes y terceras personas. Los siguientes recursos son ejemplos de información Pública:

- Los folletos que comercialización, los anuncios hechos en la prensa, folletos de reclutamiento.
- La dirección de la empresa y números de teléfono
- La información disponible en el Web.

3.2.2. Políticas

La Aplicación de esta política sigue los procedimientos definidos en el Proceso de clasificación de los registros vitales:

- La Información se protegerá a lo largo de su ciclo de vida y de una manera correspondiente con su categoría de clasificación que incluye almacenamiento y prácticas de disposición de la misma.
- No debería ser práctico etiquetar algunos tipos de información, aun cuando muy clasificado estos sean. Por consiguiente se piensa que el etiquetado electrónico de información se aplica principalmente a los documentos. El volumen de datos del cliente, el código fuente, y otro binario o datos leíbles

por máquina no pueden etiquetarse pero siempre serán manejados según el proceso de clasificación de los registros vitales.

- Los sistemas de e-mail no permitirán o no se configurarán para que envíen automáticamente desde las direcciones electrónicas de SINet a direcciones que no sean de SINet. Esto es para evitar que el correo electrónico confidencial sea observado por personal de sistemas que no sea de Omnes.
- Los sistemas de computación son clasificados según los datos que ellos contengan, guarden, o procesen, serán físicamente protegido con los controles de acceso apropiados para esa categoría de clasificación otorgada.
- La degradación de la información, que es una categoría de clasificación sólo se hará con el permiso del dueño de los datos.
- La perdida o descubrimiento inadecuado de información se informará al Funcionario de Seguridad de Sitio.
- Se usarán mensajeros garantizados para transportar información secreta ó confidencial y no medios electrónicos.
- La Información Secreta y Confidencial, no será leída, discutida, o expuesta en los aviones o en los restaurantes, ascensores, baños, u otro lugar público dónde pueda ser oída por casualidad. Esto incluye las conversaciones por teléfono.
- La información Confidencial no puede discutirse en los circuitos de voz de alto riesgo como teléfonos de hotel, teléfonos públicos, teléfonos no GSM, teléfonos móviles, o situaciones dónde los competidores pueden estar presentes, esto para prevenir ser escuchados detrás de las puertas y llamadas supervisadas.

3.2.2.1. Requisitos de Interacción con terceras personas

- Pueden darse a Terceras personas el acceso a la información Confidencial y Privada de Omnes cuando exista una necesidad demostrable y sólo cuando el dueño de la información apruebe su descubrimiento.

- Un acuerdo firmado de no descubrimiento es requerido antes de que se descubra la información privada o confidencial de Omnes por terceras personas.
- Al remitir la información por empleados que no son de Omnes, ellos notificarán la categoría de la clasificación y la protección apropiada que deberá aplicarse, como se indica en el formulario de acuerdo contractual.
- Se tratarán documentos secretos de terceras personas de acuerdo con la categoría de clasificación de Omnes o la próxima categoría más alta.

3.2.2.2. La autenticación y Requisitos de la Transmisión

- El Acceso a la información Confidencial de Omnes exigirá la autenticación PKI para acceder.
- Toda información de contraseñas es considerada confidencial de Omnes y será encriptada durante una transmisión.
- Las contraseñas internas de Omnes (como la contraseña de acceso al Directorio Corporativa) no pueden usarse para autentificarse a servicios externos a SINet.
- Durante una transmisión de información Confidencial o Secreta de Omnes será protegida con métodos de encriptación durante la transmisión. La información del cliente considerada confidencial puede transmitirse sin encriptarse en las conexiones privadas, punto a punto con la red del cliente con el consentimiento del cliente.

3.2.3. Funciones y Responsabilidades

Individuos o departamentos pueden tener papeles y responsabilidades múltiples.

El Funcionario principal de la Información: El Funcionario principal de la Información es responsable de promulgar la información de las políticas de clasificación de información de Omnes, normas, y procedimientos.

El Dueño de Información comercial: Establecer la propiedad comercial es importante por dos razones: 1) la Información es crítica para la unidad de negocio y es a menudo compartido por la corporación. 2) aplicaciones que afectan la información corporativa serán planeadas y manejadas a un nivel de convicción de garantía de calidad más alto y coordinado por cada área comercial para lograr el

máximo beneficio en el negocio. El Gerente de la Unidad Comercial tiene el papel de Dueño de Información Comercial (BIO) y es finalmente responsable por las reglas la definición circundante, colección, uso, y disposición de información comercial. Las funciones de BIO pueden delegarse, pero el resto de Gerentes de Unidades Comerciales son responsables para el papel. El BIO proporciona la dirección general a la unidad comercial para ayudar a derivar la mayoría de beneficios de información que recoge las inversiones, y también debe:

- Asegurar la clasificación apropiada de datos corporativos;
- Aseguran la implementación de procesos para controlar el acceso del usuario y autorización de datos comerciales;
- Asegurar la implementación de procesos para mantener la integridad, la disponibilidad, la exactitud, la precisión, la consistencia, la estandarización, y valor de los datos;
- Definir y asegurar el entrenamiento apropiado del personal y otros para asegurar que los datos sean capturados y se usen con precisión, eficacia.
- Entender y promover el valor de los datos para los propósitos de expansión de la compañía y asegurar que las necesidades de las unidades de negocio sean representadas en todos sistemas de información en su desarrollo y despliegue.
- Asegurar el cumplimiento de los requisitos de privacidad y otra legislación.

El Dueño de los datos: El dueño de los datos son los empleados, gerentes comerciales, o terceras personas asociados con cada recurso de información o grupo del recurso (incluso la información pública). Típicamente es la Gerencia de una línea comercial y, una función administrativa, se agrupan y están a un nivel dirigiendo, creando, procesos o manejos de datos para lo cual ellos son responsables.

Los dueños de datos son responsables para:

- La clasificación inicial y etiquetado de recursos de datos;
- Revisar la clasificación y etiquetado, periódicamente o cuando los recursos de información lo exijan;
- Valorar el balance de los datos;

- La definición de requisitos procesales para el acceso de información, autorización del usuario, y mantenimiento de integridad de datos, disponibilidad, y confidencialidad; y comunicación de esos requisitos a los Administradores de Datos, proveedores de servicios, y usuarios;
- La delegación de responsabilidades para la protección a los Administradores de Datos y vigilancia de actividades cotidianas;
- La participación en el análisis de riesgos, con respecto a los recursos de información y sus protecciones.

Los Administradores de datos: La Unidad de Sistemas (IT), gerentes de las líneas de negocio, y el administrador de funciones actuales son los Administradores de Datos. Ellos dirigen la creación, proceso, o manejo de datos y son responsables de:

- El desarrollo e implementación de controles procedimentales basados en los requisitos de los dueños de los datos
- Asegurar que las fuentes de información sigan los procedimientos, normas y políticas de seguridad de Omnes;
- Mantener el entrenamiento necesario para llevar a cabo la norma;
- Asegurar que los planes de recuperación de desastre existan y sean viables;
- Informar a los Dueños de Datos y BIO cualquier variación de las políticas, normas, o procedimientos y en cualquier pérdida de información confidencial, integridad, o disponibilidad;
- Participar en el análisis de riesgo con respecto a los recursos de información y su protección.

Los usuarios: Los usuarios de los recursos de información son individuos que tienen el permiso para acceder y usar los datos, si escriben o están implícitos para los propósitos comerciales. Es fundamental que todos los niveles de la empresa se aseguren que todos los usuarios de datos dentro de su área son conscientes de sus responsabilidades como está definido en esta política. Los usuarios son responsables para:

- Conocer y obedecer los procedimientos y políticas de clasificación de Omnes;
- Administrar las responsabilidades de los recursos de información de Omnes;
- Proteger la información de acuerdo con su clasificación;
- El acceso a datos hecho a través de la cuenta del usuario y el uso subsecuente y distribución de los datos;
- Cumplimiento con los requerimientos locales y corporativos en la privacidad y otros estatutos pertinentes.

Los usuarios se prohíben de:

- Usar los datos para su propia ganancia personal o ganancia de otros;
- El descubrimiento de datos por parte de personas desautorizadas sin el consentimiento del Dueño del Datos.

3.3. PROCESO DE CLASIFICACIÓN DE LOS REGISTROS VITALES

Se exigen a todos los empleados de Omnes y a subalternos de contratistas que protejan información propietaria poseída por o bajo la custodia de Omnes, y para mantener la confidencialidad de esta información propietaria. Las regulaciones de la clasificación se aplican a todo Omnes, y a toda la información creada, sin tener en cuenta los medios de comunicación, almacenamiento, o transmisión dentro de esos negocios.

La norma vigente define al sistema de clasificación dispuesto en cuatro niveles: Público, Privado, Confidencial, y Secreto. Omnes clasifica información y valores materiales exclusivamente en base a la confidencialidad. Otros aspectos de seguridad básicos de integridad y disponibilidad no son parte del esquema.

Esta norma técnica describe cómo identificar el nivel de clasificación correcto y aplicar la protección apropiada. El nivel de clasificación determina cómo el recurso se etiqueta y se protege basado en el riesgo de su descubrimiento. Por consiguiente la norma técnica especifica a los usuarios que se ocupan de las

instrucciones así como la facilidad de controlar áreas de trabajo, lugares de almacenamiento, alojamiento, etc.

3.3.1. El papel de cada uno de los Funcionarios

El Dueño de Información comercial (BIO)

En el papel de BIO, los Gerentes de la Unidad Comerciales son responsables en comenzar y mantener los esfuerzos para aplicar estas políticas (políticas para los registros vitales) a sus funcionamientos comerciales. La informática y funcionamientos abarcan muchas situaciones únicas donde el juicio y entendiendo de riesgos deben aplicarse para asegurar confidencialidad de información secreta.

El Dueño de los datos: Las líneas del producto deben identificar sus recursos de informática o tipos del recurso. Deben asociarse un dueño de los datos con cada tipo de recurso identificado. El Dueño de los datos es responsable para la clasificación apropiada (incluso la revisión de la clasificación) y por asegurar los requisitos de esa protección y se especifica al Administrador de Datos asociado.

El Administrador de los datos: Gerentes de Sistemas y administradores son responsables para llevar a cabo los procedimientos de control y por proteger los recursos según los requisitos del Dueño de los datos y políticas de Omnes.

3.3.2. Especificaciones de Recursos de información que se controla y se maneja

Deben ponerse los controles apropiados en el lugar para cada categoría de la clasificación. Estos deben equilibrar facilidad de uso, los costos de protección, y las necesidades de protecciones. La pérdida de control de la información puede prevenirse por dos cosas:

- definiendo el nivel de control apropiado a cada tipo de información,
- los mecanismos apropiados desplegados para llevar a cabo el nivel deseado de control.

La siguiente tabla traza el nivel de clasificación (la confidencialidad de recursos) a los mecanismos de control que deben aplicarse para proteger esa confidencialidad. El nivel predefinido mínimo de Clasificación para cualquier nuevo documento es Privado de Omnes.

TIPO DE RECURSO	SECRETO	CONFIDENCIAL	PRIVADO	PÚBLICO
Forma de Etiquetar	Marcado: Omnes Secreto	Marcado: Omnes Confidencial	Marcado: Omnes Privado	Marcado: Omnes Público
	El correo electrónico: Se añada al e-mail pie de página o línea de la firma.			El e-mail: Ninguna etiqueta es requerido
	Los Medios de comunicación trasladables: Escribir a mano sobre la etiqueta y adherirla en los medios de comunicación trasladables o imprimir una etiqueta y adherirla a los medios de comunicación trasladables. Documento Electrónico: Agregue al documentar el pie de página. Documento Impresos: Agregue al documentar el pie de página			
El Control de Acceso	La información estará disponible para las personas que	Disponible en un base de conocimientos de lo más básico. Seguridad de autentificación	Un registro de todos los accesos realizados	Ninguna restricción

TIPO DE RECURSO	SECRETO	CONFIDENCIAL	PRIVADO	PÚBLICO
	han sido asignadas. Autenticación PKI es requerida. El dueño de los datos debe especificar los derechos explícitos de acceso	segura requerida (vía PKI o contraseña). El dueño de los datos puede especificar derechos de acceso explícitos.		
Almacenamiento: Medios de comunicación Fijos	Siempre encriptado. Remover todas las copias descifradas. Almacenar solo en un sistema secreto de Omnes. No almacenar en PDA	Encriptar cuando sea posible. Remover todas las copias descifradas. Almacenar solo en un sistema confidencial de Omnes.	Sólo almacenar en un sistema Privado de Omnes	Ninguna restricción
Almacenamiento: Trasladable	Electrónico: Siempre encriptado. Físicamente	Electrónico: Encriptado cuando sea posible. Físicamente	Electrónico: Almacenar en una área Privada de	Ninguna restricción

TIPO DE RECURSO	SECRETO	CONFIDENCIAL	PRIVADO	PÚBLICO
	seguro en un área secreta de Omnes. Almacenamiento Offsite: Los medios de comunicación electrónicos debe ser encriptados y estar en un casillero cerrado con llave. Los medios de comunicación en papel no deben existir.	segura en una área confidencial de Omnes. Almacenamiento Offsite: Papel y medios de comunicación en un casillero cerrado con llave. El dueño de la información puede especificar el requisito para encriptar archivos, datos, o respaldos.	Omnes Almacenamiento de Offsite: Almacenar en un casillero cerrado con llave	
Transmisión	Archivo/e-mail: Encriptar para los destinatarios. Incluir las instrucciones de	Archivo/e-mail: encriptar para los destinatarios cuando sea posible	Encriptar para las conexiones de red que no pertenezca a SINet.	Ninguna restricción

TIPO DE RECURSO	SECRETO	CONFIDENCIAL	PRIVADO	PÚBLICO
	manipulación / almacenamiento en el mensaje. Otros: Haber encriptado las conexiones de red requeridas. El dueño debe especificar los requerimientos de encriptación	Otros: Haber Encriptado las conexiones de red requeridas. El dueño puede especificar los requisitos para la encriptación de archivo o datos.		
Enviando	Los Medios de comunicación físicos: Prohibido. Ver la impresión. Los Medios de comunicación electrónicos:	Los Medios de comunicación físicos: Mensajero Garantizado. Los Medios de comunicación electrónicos: La encriptación cuando sea posible.	Los Medios de comunicación físicos: Mensajero Garantizado Los Medios de comunicación electrónicos: Encriptado	Ninguna restricción

TIPO DE RECURSO	SECRETO	CONFIDENCIAL	PRIVADO	PÚBLICO
	La encriptación es requerida. La confirmación electrónica requerido.		cuando sea posible.	
Disposición	E-mail: Borrar del buzón y de la carpeta de reciclaje. Papel: Destrozar en un máquina de papel. Archivos del disco: Realizar un borrado físico y lógico. Floppys: Destruirlos CD's: Romperlos o borrar por	E-mail: Borrar del buzón y de la carpeta de reciclaje. Papel: Destrozar en una máquina de papel. Archivos del Disco: Realizar un borrado físico y lógico. Floppys: Destruya o formatéelos 7 veces. CD's: : Romperlos o borrar por microondas	Papel: Destrozar en una máquina de papel. Los CD: Romperlos (de manera segura)	Ninguna restricción

TIPO DE RECURSO	SECRETO	CONFIDENCIAL	PRIVADO	PÚBLICO
	microondas			
Impresión / Copiando	Impresión / Copiando PROHIBIDO excepto temporalmente por encontrarse en una presentación. TODO el material impreso debe destruirse inmediatamente para el siguiente evento.	En la área Confidencial o Privada de Omnes, asistida por el destinatario o creador.	En una área Privada	Ninguna restricción
Presentación	En una sala de reunión Confidencial	En una sala de reunión Confidencial	En una sala de reunión Privado	Ninguna restricción
Reclasificación	Por el dueño de los Datos o el Administrador delegado	Por el dueño de los Datos o el Administrador delegado	Por el Dueño de los Datos	Por el Dueño de los Datos

Cuadro 3.1 Clasificación de la información

3.3.3. Etiquetado de Información

Toda información creada recientemente relacionada al negocio de Omnes, debe seguir el principio de la Norma de clasificación de Seguridad de la Información, la misma está a sujeta a la clasificación. Esto incluye una contestación o envío de alguien más por correo electrónico.

- Deben etiquetarse sólo documentos electrónicos o impresos humano-leíbles. Algunas excepciones existen como archivos de código fuente que deben etiquetarse propiamente para protección de los derechos de propiedad intelectual.
- Los datos del cliente, en el formulario impreso, no se exige ser etiquetado, a menos que sea requerido por el cliente, sin embargo otros estándares de almacenamiento y manejo para el nivel de la clasificación se aplican.
- El etiquetado del documento se facilitará por un Addin personalizado por las aplicaciones de Microsoft Office. El Addin proporcionará la colocación automatizada de una etiqueta de la clasificación, menú contextual de consejos de manejo del documento, y cambios a las propiedades del documento. El Addin se entregará como parte de la Imagen Normal o disponible del Servidor de distribución de software de Omnes.
- Documentos PDF creados a partir de los documentos MS Office heredarán algunas de las propiedades y etiquetas visibles.
- El correo electrónico público es el único tipo del documento que no requiere una etiqueta.

3.3.4. Estructura de una Etiqueta

La etiqueta visible, se insertó manualmente o con el MS Addin, usará la siguiente sintaxis:

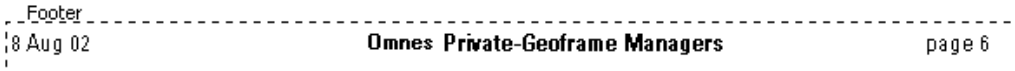
La Categoría de Omnes [- la extensión es optativa]

Donde

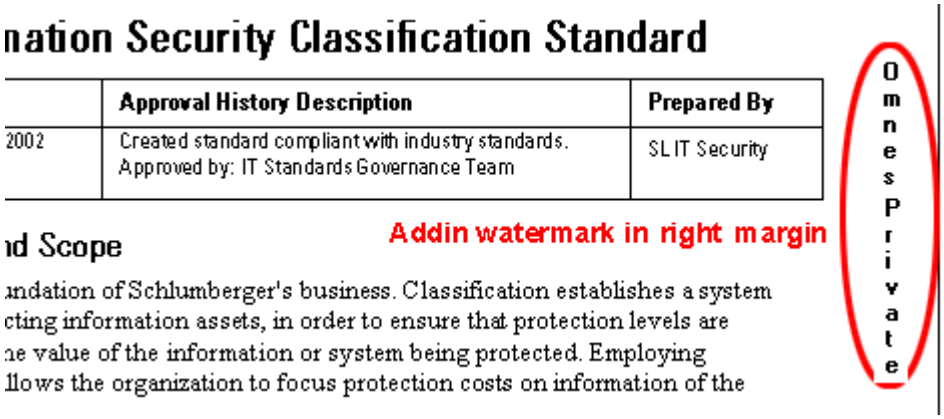
La categoría = Pública, Privada, Confidencial, o Secreta.
La Extensión es optativa = Etiquetas registradas con la unidad comercial

Los siguientes ejemplos muestran dos situaciones para agregar una etiqueta. El Addin evita los conflictos con los pies de página de página existentes en Word y PowerPoint poniendo una marca de agua en el margen derecho. Al etiquetar manualmente, cualquier situación es aceptable.

Ejemplo 1: la entrada del pie de página Manual



Ejemplo 2: Addin el watermark automático

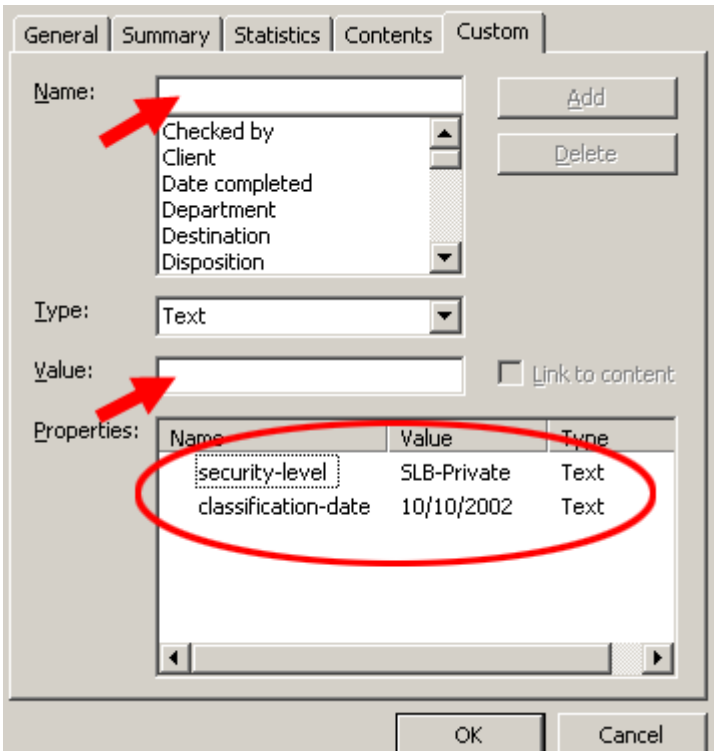


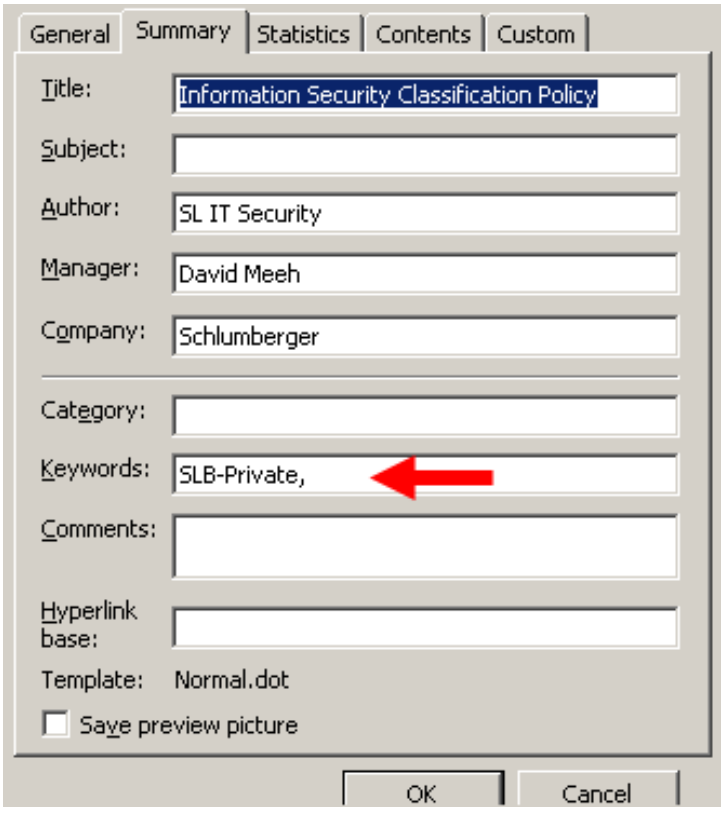
3.3.5. Propiedades en un documento de Office

Si ajustó manualmente o con el Addin, cada documento de MS Office tendrá una etiqueta de clasificación y la fecha agregado en el archivo de la ventana de propiedades.

1. En la ventana de Propiedades, haga clic en etiqueta Personalizada.
2. En el campo de Nombre ingrese **el nivel de seguridad**.
3. En el campo de valor ingrese **la Categoría de Omnes [-la extensión es optativa].**
4. Haga clic el botón **Agregar**
5. En el campo Nombre ingrese **la fecha de clasificación**
6. En el campo de Valor ingrese **DD/MM/YYYY** (día/mes/año)
7. Haga clic en el botón **Añadir.**
8. Haga clic en la etiqueta Resumen.
9. En el campo de la Palabra clave ingrese **la Categoría de Omnes [- la extensión es optativa]**

El paso 9 asegúrese que si el archivo es convertido a formato PDF, la información de la clasificación será visible, desde los campos palabra clave serán llevados a través de la conversión. En el siguiente ejemplo, usted puede ver los ejemplos de configuración para las etiquetas personalizada y resumen:





3.3.6. La Etiqueta Meta en archivos de la Web

En los archivos de la Web use la etiqueta metadata con el nombre y contenido de parámetros, como se muestra debajo:

<head>

<meta name="security-level" content=" la Categoría de Omnes [- la extensión es optativa]>

3.3.7. Almacenamiento

Los requisitos de almacenamiento se aplican a la información para la cual usted es quien va a custodiarla. Un gran cuidado debe tenerse con el almacenamiento de información Secreta y Confidencial.

- Máquinas que guardan la información Confidencial o Secreta deben adherirse a las normas de clasificación de información.
- El almacenamiento de medios de comunicación trasladables o removibles deben ser altamente asegurados y supervisados.
- El almacenamiento Off-site de los medios de comunicación deben ser asegurados apropiadamente dentro de las facilidades de almacenamiento y no debe contarse solamente con controles de medios Informáticos.

3.3.8. Transmisión y Encriptación.

Los requisitos de transmisión se aplica a algo que usted envía, si o no usted creara la información. Esto incluye el uso de servidores de aplicaciones para transferir datos así como las aplicaciones de escritorio.

- La transmisión dentro de una red de información de contraseñas siempre debe encriptarse.
- Si la parte receptora no tiene la tecnología para recibir y descifrar su transmisión, otros medios deben usarse para asegurar la entrega segura. En el caso de un archivo vinculado a un correo electrónico encriptado recibido por un usuario de PC normal de Omnes, usted puede seguir este proceso:
    - Descifre el archivo.

- Vuelva a encriptar usando una llave simétrica confiable. Esta función está disponible dando clic derecho en el archivo y seleccionando en el menú option Entrust Advanced-> Password Protect.
- Enviar el archivo SIN la contraseña.
- Comunique la contraseña, normalmente por conversación telefónica directa con el destinatario.
- Aconséjele al destinatario que use el Entrust "Protección por Contraseña" utilidad de desencriptación disponible en http://www.entrust.com/passprotect/

- Al remitir información Secreta, Confidencial, o Privada, de Omnes el remitente es responsable de cumplir el acuerdo de no descubrimiento por terceras personas u otros acuerdos del contrato, y que éstos acuerdos especifican las pautas de manipulación para los documentos secretos de Omnes.
- Los siguientes métodos de encriptación o protocolos son aceptados para el uso interior. Los requisitos del cliente para la encriptación son tomados según sus requisitos.
  - La Encriptación de Archivos “E-mail”: Claves confiables asimétrica o simétrica (protección por contraseña)
  - La Comunicación de las aplicaciones: Se usa un túnel Seguro que usa la encriptación más fuerte permisible por las regulaciones locales (128 bits es suficiente actualmente). Los túneles pueden usar SSH, TLS u otro método basado en SSL, o IPSec.
  - Telnet y FTP: Se reemplazan con la distribución normal SSH y aplicaciones de SecureCopy. Se usa certificados, en lugar de la autenticación por contraseña.
  - Las aplicaciones sin Encriptación: Las aplicaciones que no pueden encriptar la información Confidencial y Secreta deben usarse por separado, punto a punto, en los medios de la red privada (por ejemplo las aplicaciones DMC).
  - En una Jornada completa o Enlaces de comunicación que demanda una conexión: Usar IPSec

3.3.9. Clasificación de los Sistemas

Un sistema es una máquina capaz de guardar la información, como un PDA, computadora portátil, servidor de Web, o servidor de la base de datos. La Clasificación de los sistemas está basada en la información que éstos contengan. Un sistema con una base de datos o la aplicación asumirá el nivel de clasificación más alto que la información generada o brindada por las aplicaciones en el sistema. Los sistemas de Omnes no requieren etiquetado.

Lo Privado de Omnes: Todas las máquinas de Omnes tienen instalados el software Standard Image v3.5 y versiones anteriores, son clasificadas como privado de Omnes por defecto. Ese estándar de las máquinas tiene una apropiada configuración de seguridad incorporada. PCs no estandarizados y todos los servidores deben cumplir con el arreglo de seguridad mínimo descrito en requerimientos del sistema.

Lo Confidencial de Omnes: Todo los PDAs, PCs, y servidores que procesan y almacenen datos Confidenciales de Omnes se adherirán a lo aplicable sobre requerimientos del sistema y residirán en una área de trabajo Confidencial o de almacenamiento de Omnes.

- Autenticación del usuario vía PKI o Contraseñas confiables Seguras son requeridas. Todos los métodos de autenticación deben ser seguros con certificados o contraseñas encriptadas.
- Debe quitarse Telnet y FTP o ser reemplazados con SSH y SecureCopy.
- La información confidencial será encriptada durante la transmisión y, dónde sea posible, durante el almacenamiento.
- Estos sistemas deben manejarse, administrados, parchados, y mantenidos por personal con entrenamiento en seguridad y la certificación reconocida por Omnes. Los Dueños de los datos pueden requerir chequeos de fondo.

Lo Secreto de Omnes: Todos los PCs, estaciones de trabajo, y servidores que procesan y almacenan datos secretos de Omnes se adherirán a lo aplicable en requerimientos del sistema y residirán en una área de trabajo o de almacenamiento Confidencial.

- Estos sistemas deben ser altamente asegurados y muy resistentes a la penetración ante un ataque, y deben encontrarse dentro de un perímetro de seguridad controlada vía red.
- Procedimientos de monitoreo altamente eficaces también deben estar en el lugar para detectar el acceso desautorizado, y deben realizarse pruebas regulares de penetración.
- Se requiere autenticación de insignia corporativa PKI para el acceso del usuario, y todos los métodos de autenticación deben ser confiables (contraseñas encriptadas o certificados).
- La información secreta se encripta durante la transmisión y almacenamiento.
- Los usuarios de máquinas portátiles deben adherirse a las normas del almacenamiento para este nivel de clasificación y deben emplear la protección de un cortafuego personal o dispositivo de cortafuego al conectarse a la red de la misma manera que a SINet. PDAs nunca deben guardar la información secreta, incluso encriptada.
- Debe quitarse Telnet y FTP o deben reemplazarse con SSH y SecureCopy.
- El acceso administrativo se restringirá a vigilantes designados por los dueños de los datos quienes deben mantener un entrenamiento en seguridad y tendrán una certificación reconocida por Omnes.
- Chequeos de fondo (educativo, historial del trabajo, las referencias delictivas, referencias personales, financieras) estas indagaciones se las debe realizar dos veces anualmente.

3.3.10. Conferencia en línea

Estos requisitos se aplican a las conferencias electrónicas únicas de Omnes así como reuniones con terceras personas que hacen uso de la red interna de Omnes.

Lo Privado de Omnes: El sólo uso de cualquier de los servicios de colaboración electrónica básico de Omnes.

Omnes Confidencial y Secreto

- El sólo uso de cualquier servicio de colaboración electrónico básico, con encriptación en la red y la autenticación segura habilitado y requerido.
- El uso referencial de auditoria y responsabilidad para las acciones del usuario (no el contenido de la información).
- Anotar las sesiones, con la mayor retención posible por un periodo no mayor de tres meses, para los siguientes detalles: los participantes, la fecha/hora, dirección IP (a través del navegador), duración de conexión, la información transferida o transmitida.

3.3.11. Facilidad de Controles

Los lugares de trabajo como un conjunto no son clasificados como Privado o Confidencial, pero el trabajo que tiene lugar en dicho sitio puede ser clasificado como tal. Esta sección describe donde y cómo dirigir el trabajo clasificado. El propósito de clasificación del sitio es no anunciar con señales donde encontrar datos sensibles, pero para controlar el acceso a las tales áreas.

3.3.12. Zonas de trabajo

Por defecto todos los sitios de trabajo de Omnes no son clasificados como Privado, pero si un empleado trabaja principalmente en datos confidenciales, su área de trabajo debe cumplir con los requerimientos de confidencialidad que se describe a continuación. En áreas poblados por múltiples empleados que estén trabajando en una mezcla de datos Privados y Confidenciales, demostrar discreción. Puede ser prudente para crear un área separada que cumpla con los requerimientos de Confidencialidad. El administrador de la locación y grupos tales como Recursos Humanos, Contabilidad, y departamento Legal son la mayoría que requieren trabajar en áreas separadas. Además para especificar los requerimientos de clasificación listados a continuación las siguientes reglas generales.

- La clasificación de señales solo en el perímetro del sitio. Los puntos de entrada y salida deben ser marcados “Omnes Private”.
- No marcar las áreas de trabajo Confidenciales, pero requerir de controles de acceso.

- Los Consultores de Omnes que trabajan fuera del sitio deben obedecer todas las reglas del área de trabajo.

Público de Omnes: Las áreas públicas que actúan como puntos de facilidad de entrada principales, como las áreas de la recepción, necesitan sólo desplegar el logotipo de Omnes; ninguna otra señal de clasificación. En la entrada principal debe asistirse cuando no cerró con llave. Cuando se cerró con llave, el acceso del empleado debe controlarse vía la Insignia Corporativa, teclado pequeño, o la llave personal.

Privado de Omnes: Esa señal debe aparecer en lo que es propio o rentado de Omnes, en la entrada y salida de las Locaciones. Las señales deben cumplir las pautas de identificación de Omnes en tamaño y color del logotipo comercial.

Confidencial y Secreto de Omnes: No anuncie las áreas Confidenciales. Tales áreas deben localizarse dentro del perímetro del área Privada de Omnes. El control de acceso debe restringirse; un control mínimo se requiere una cerradura y un sistema de control de acceso con un registro de poseedores de la clave es importante. Para el alto tráfico en las áreas de cómputo o centros de procesamiento de datos, y para áreas usadas por múltiples empleados, la cerradura y claves de acceso deben ser reemplazadas por un sistema de entrada por Insignia Corporativo. Pueden usarse los cuartos de Conferencias para dirigirse a negocios públicos, privados, y confidenciales tanto tiempo como las características de seguridad requeridas puedan ser activadas o puedan reforzarse. Etiquetar no es requerido.

Lo privado de Omnes

- Asistentes deben presentar una Insignia Corporativa u otra identificación de Omnes (por ejemplo un Pasaporte de QHSE). El gerente en la reunión es responsable de asegurar que los asistentes son los apropiados. Use las facilidades que presta Omnes en lo posible.
- Si es usado un centro de conferencias en un hotel o en algún otro lugar que no corresponda a Omnes, el área debe cerrarse con llave mientras no

esté prestando sus servicios. El área puede permanecer abierta durante la conferencia, pero con las puertas cerradas.

- Quitar toda la información del área al final de la conferencia. No use el basurero del hotel o alguna otra facilidad del mismo para los residuos o material que se utilizo para la exposición.

Lo Confidencial y Secreto de Omnes

- Deben invitarse a los asistentes. Los asistentes deben presentar una Insignia Corporativa u otra identificación de Omnes (por ejemplo un Pasaporte de QHSE).
- Un ayudante de la reunión debe registrar la asistencia en la puerta, chequeando la asistente por identificación, prevenga las interrupciones inesperadas, y por otra parte asegure la confidencialidad. El ayudante de la reunión debe permanecer en la entrada a lo largo de la duración de la reunión. Deben coordinarse cambios del último minuto en la lista del asistente entre el presidente de la reunión y el ayudante de la reunión.
- El área debe ser autónoma, con cuatro paredes y una puerta cerrada con llave. Use las facilidades de Omnes siempre que sea posible. Una facilidad que no sea de Omnes debe reunir todos los requisitos.
- Quite toda la información en el área que se utilizo al final de la conferencia.

3.3.13. Los medios de la red

Una red no está clasificada por la información transmitida, pero según la importancia que Omnes otorgue como un medio de comunicación su clasificación puede variar. En este contexto, una red está definida como la conectividad electrónica entre dos lugares e incluye hasta lo último para la realización de una conexión: equipo, armario, cuartos de la red o puntos de terminación de red. Las redes se las clasifica en dos categorías:

Lo Privado de Omnes: Incluye la interfaz de los puntos de acceso a la red LAN SINet, o puntos de red con el acceso hacia SINet. No hay ningún requisito de etiquetar.

Omnes Confidencial y Secreto: Incluye toda la infraestructura de la red WAN y LAN de SINet , que incluyen todos los armarios de la red o los sistemas Confidenciales. Los sistemas confidenciales no deben ser localizados en áreas desatendidas. Marque al área como Confidencial de Omnes y liste cualquier otro aviso de restricción requerido por ley local. Si el acceso a las tales áreas es poco frecuente, por ejemplo un armario de la red, los sistemas de control de acceso electrónicos no pueden ser muy útiles. En la ausencia de control de acceso electrónico, asegure con una cerradura y el sistema de claves con los poseedores de las claves registrados debidamente.

3.3.14. Zonas de almacenamiento

Los siguientes son los requisitos de almacenamiento que se aplican a equipos, medios de comunicación, y documentos.

Privado de Omnes: Las áreas del almacenamiento para los artículos de oficina y las partes de repuesto usadas para operaciones en general. No es necesario etiquetar. El gerente de la locación puede elegir en cerrar con llave tales áreas para controlar costos.

Omnes Confidencial y Secreto

- Deben marcarse como confidencial de Omnes los medios de comunicación o áreas de almacenamiento de documentos, deben cerrarse con llave, y debe restringirse el acceso solamente a personal autorizado. Cerradura electrónica o de llave y control de acceso por claves es aceptable.
- Los arreglos contractuales con los proveedores deben especificar los requisitos del almacenamiento apropiados para la información, medios de comunicación, u otra información confidencial del Cliente o de Omnes. Los dueños del contrato deben verificar el cumplimiento periódicamente vía auditoria física.
- El almacenamiento Off-site de medios de comunicación requiere de almacenamiento en contenedores asegurados separadamente. El personal de almacenamiento no debe tener el acceso a los volúmenes del recipiente. Los Dueños de los datos pueden requerir encriptación de ciertos recursos. La encriptación y las llaves físicas deben permanecer en la

posesión de empleados autorizados. Deben anotarse todas las transacciones con los medios de almacenamiento y un inventario de los contenedores mantenidos en almacenamiento.

3.4. RECLASIFICACIÓN DE LA INFORMACIÓN

La reclasificación debe hacerse por el Dueño de los Datos o del Administrador de los Datos asignado. El BIOs debe asignar al nuevo Dueño del Datos, y los Dueños de los Datos deben designar Administradores que pueden reclasificar así como designar tipos de información sobre la cual ellos tienen este privilegio. Sólo los Dueños de los Datos pueden reclasificar la información Confidencial o Secreta.

Los Dueños de los datos pueden reclasificar información basada en la edad, valor, obsolescencia, o sanear (quitar de referencias técnicas o referencias personales). La Reclasificación en edad puede ser automática y se puede hacer un buen uso de extensiones unidas con guión a los cuatro estándares de categorías. Muchas veces la información de anuncios Públicos puede ser severamente clasificada hasta que sea liberado. Esto puede incluir anuncios de productos, el nivel financiero, o planes de adquisición o de despojo.

Si usted cambia o incluye información clasificada en su trabajo, su versión está sujeta a la clasificación actual y a todos los requisitos de clasificación de Omnes para etiquetar, almacenar, impresión, y transmisión es decir a todo nivel de clasificación.

Cualquier información de Omnes se reclasifica por el Dueño de los Datos (por ejemplo, la documentación que es hecho para el público cuando un producto es liberado comercialmente) debe adherirse al etiquetado apropiado, acopio, impresión, y transmitir los requisitos para el nuevo nivel de clasificación. La mayoría de reclasificación involucrará mudanza de información Secreta y Confidencial a un nivel mas bajo, desde costos superiores asociados con mantener la información en estas categorías.

3.4.1. Extensiones de la clasificación

Pueden agregarse extensiones unidas con guión a las cuatro categorías de clasificación básicas. Las extensiones serían usadas por unidades comerciales o medios de R&D que requieren más granularidad para la clasificación en un negocio específico. Las extensiones son optativas, y si usó es asignado por el BIO o Dueño de Datos.

Las extensiones podrían tomar el formulario de una fecha de expiración, el nombre del dueño, o podrían indicar la restricción de NDA. Las extensiones pueden ser útiles para restringir el acceso a la información. Estos controles deberían ser entonces descritos y ser comunicados al Administrador de Datos. Los requisitos mínimos para cada categoría primaria son especificados en esta norma. Sólo pueden usarse las extensiones para añadir manejo adicional, almacenamiento, o control de requisitos a la categoría de la clasificación primaria y no pueden usarse para relajar cualquiera de los controles especificados en esta norma.

3.4.2. Pautas

- Cuando haya duda sobre el nivel de clasificación, pregúntele a su superior.
- Proteger la Información es más importante que etiquetar la información.
- Antes de enviar información, pregúntese si el destinatario sabrá como manejar su información. El remitente es responsable para la clasificación.
- Antes de guardar la información, pregúntese si otros entenderán la importancia de esta información cuando la logren recuperar.
- Antes de hacer una presentación, Esté seguro que las diapositivas estén etiquetadas para que el público no pase la información a los competidores. El expositor es responsable por su clasificación.
- El correo electrónico confidencial recibido de un cliente debe manipularse apropiadamente mientras está en su posesión. Mantenga la información encriptada en el sistema de Omnes.
- No encriptar todo. La encriptación sólo debe aplicarse como está descrito en esta norma.

- Si usted esta inseguro sobre que si el legado de la información es Confidencial, guárdelo en una carpeta segura. El legado de la información no requiere el etiquetado, pero requiere una manipulación apropiado.

3.4.3. La Seguridad General

El uso excesivo o inapropiado de los medios informáticos, incluso el ancho de banda de la red, para el uso no comercial se prohíbe. Bajo ninguna circunstancia tales medios se usarán para la ganancia financiera personal, solicitar otros para actividades no relacionados al negocio de Omnes, o en relación con campañas políticas o cabildeando. El departamento de personal (los Recursos humanos) puede hacer disponible o pueden autorizar boletines de anuncios de propósito especial y páginas Web para los empleados puedan comercializar y vender sus propiedades personales y para anunciar eventos sociales aceptados por Omnes y otras actividades permitidas.

Además de la complacencia con orientación de seguridad que entrena las reglas, los usuarios deben:

Tomar los pasos razonables para proteger los valores materiales del robo. Esto incluye pero no se limita a los disquetes, licencias del software, computadoras portátiles, módems, tarjetas de acceso físicas, tarjetas inteligentes, y otros dispositivos periféricos.

Use las herramientas autorizadas por Omnes para la encriptación de la información de Omnes. Siga las regulaciones criptográficas de Omnes.

No descubra información técnica o comercial confidencial esto está dirigida para personas ajenas a la empresa o personas desautorizadas, incluyendo pero no limitado a datos, números de acceso telefónico a la red, los protocolos de comunicación, los números de identificación personal, contraseñas, procedimientos de registro, y sistemas de correo de voz.

No use computadores de la red de Omnes para penetrar a obtener información o romper la seguridad de cualquier otra red

El sistema de Omnes, no utilizarlo para obtener acceso desautorizado a sistemas de información de cualquier otra persona, cuentas, o equipo a menos que expresamente la parte de su definición de funciones (por ejemplo como parte de seguridad de la información), se lo permita, y sólo dentro de SINet.

No escriba intencionalmente o distribuya cualquier código de software diseñado para auto diseminarse, dañe, o por otra parte la actuación posterior de o acceso a cualquier sistema de información de Omnes, red. Esta política incluye creación o experimentación con los virus, gusanos, y software similar.

Manejo de incidentes y Virus: Todas las eventualidades de seguridad serán comunicadas a una Funcionaria de Seguridad de Sitio (SSO) o Gerente del Sitio y anotado haciendo uso de la herramienta electrónica de informe de riesgos corporativa el. SSOs seguirá el procedimiento de manejo de casualidades SSO para procesar riesgos validados o casualidades.

Las contraseñas y fichas de acceso: Genere muy bien sus contraseñas que siguen las pautas de contraseña de Omnes. No transmita contraseñas vía correo electrónico o cualquier medio del texto legible. No comparta sus contraseñas, los números de NIP de tarjetas inteligentes, que la encriptación codifica, o fichas de acceso como la insignia Corporativa con cualquier otro empleado o persona ajena a la compañía.

El Software tercerista: Observe las obligaciones de autorización y restricciones en todo el software y material de propiedad registrado. Esto incluye cualquier restricción en software transmitido etiquetado “programa de libre distribución” o “shareware.” No ejecute software obtenido de cualquier fuente ajena a Omnes hasta que tal software sea revisado propiamente por virus, gusanos, caballos troyanos, y otras instrucciones que podrían dañar los sistemas de información de Omnes. Los administradores del sistema son responsables para proteger software tercerista y archivos anónimos. Esto limita el daño si el software contiene código malévolo. Esto también proporciona la información de seguimiento si el desarraigo de virus es necesario. Ningún software permite que se compartan datos entre una máquina de Omnes y el Internet sin el control del usuario. Los ejemplos son

Napster, Gnutella, todos los clientes de chat, o cualquier software que a futuro desvían la seguridad del cortafuego.

No use software de charla que permite la entrega a ciegas de archivos, es decir, software que permiten a alguien en una sesión de charla cargar un archivo en su sistema sin su consentimiento.

Herramientas de Antivirus: Omnes ha aprobado software de antivirus que sea instalado, activado, y regularmente actualizado en todos los dispositivos de informática conectado a la red de Omnes. Esto incluye el hogar y terceros sistemas de información. El programa de comprobación de virus se habilitará continuamente en las computadoras personales conectadas, aun cuando las máquinas se conectan intermitentemente.

El correo electrónico y las Herramientas de Navegación en el Web: Cualquier máquina que acceda a la red de Omnes y también se conecta al Internet vía un Proveedor de servicios de Internet se instalará y se le habilitará con un cortafuego personal o aparato de cortafuego. No remita correo electrónico de Omnes automáticamente a los servidores fuera de la red de Omnes. No abra o envíe tarjetas de felicitación electrónicas o archivos contenidos en éstos de contenido desconocido.

Compartir archivos y respaldos: No comparta las unidades de disco enteras. Los permisos de acceso a archivos serán configurados a un acceso mínimo y necesario; sólo los individuos que deben ver los datos específicos deben poder hacerlo, no use el software de compartir archivo como Napster o sistemas similares. Estos servicios pueden permitir un grado sorprendente de acceso para intrusos a muchos tipos de archivo en su dispositivo, a veces sin el conocimiento del dueño. Los usuarios se asegurarán que sus sistemas se respaldan de acuerdo con los Procedimientos de Seguridad de Sitio locales.

Las comunicaciones

- No pueden usarse los medios informáticos de Omnes para lo siguiente propósitos:
    - para llevar material difamatorio, discernidor, u obsceno;
    - en relación con cualquier infracción de los derechos de propiedad intelectual de otra persona (por ejemplo, los derechos de propiedad literaria);
    - de una manera que viola las condiciones de cualquier ley de telecomunicación que no autoriza la transferencia de datos de seguridad nacional (por ejemplo, leyes que tratan con la colección de datos, de protección, retiro, confidencialidad, y seguridad);
    - en relación con la violación o intentó violación de cualquier otra ley.
- Bajo ninguna circunstancia la entrega de, correo de voz, o correo electrónico que se originan en Omnes y ser una violación de la carta o del espíritu de práctica de empleo de Omnes o políticas de Acoso sexual. Ejemplos de contenido inaceptable que se incluyen:
    - mensajes sexualmente explícitos, imágenes, dibujo animados, o chistes;
    - proposiciones mal recibidas, petición para citas, o cartas de amor;
    - la profanidad, obscenidad, calumnia, o libelo;
    - las manchas étnicas, religiosas, o raciales;
    - creencias políticas o comentario;
    - cualquier otro mensaje que podría traducirse como fatiga o descrédito de otros basado en su sexo, raza, orientación sexual, edad, nacionalidad, invalidez, o creencias políticas o religiosas.
- No se usarán los medios informáticos para acceder o transmitir materiales obscenos u otro “contenido” que puede ser ilegal bajo las leyes locales. Por ejemplo, la posesión y distribución de ciertos tipos de documentación neonazi y propaganda pueden ser ilegales en Alemania, y otros países pueden imponer las restricciones igualmente en posesión o uso de otros tipos de contenidos.
- La falsificación electrónica se prohíbe estrictamente. La falsificación electrónica está definida como falsificar su identidad de forma alguna

mientras está utilizando los sistemas de comunicación electrónica. Los ejemplos incluyen pero no se limitan al uso desautorizado la dirección de correo electrónico de alguien y el spoofing IP.

- No realice copias, uso, o traslado de materiales de otra persona sin la autorización apropiada.
- El respeto de los derechos de propiedad literaria de terceras personas y la marca de fábrica exigidas en las imágenes en línea, texto, material de audio y video, software, información, e invenciones.

3.5. POLÍTICAS Y PROCESOS PARA LAS ÁREAS FUNCIONALES.

Esta política describe las responsabilidades de la administración en Omnes para la seguridad de la información. Se espera que los jefes departamentales tomen plena responsabilidad por la seguridad de la información y asegurar que serán orientadas como un problema comercial crítico para proveer directrices y recursos requeridos. Su atención está enfocada en la seguridad de información, mientras se protege el negocio existente, en demostrar las rigurosas normas de seguridad de información a los empleados así como los clientes potenciales.

Esta política se aplica a todas las unidades comerciales y agentes de outsourcing. El conjunto de políticas de seguridad de información define las medidas requeridas para proteger los recursos de información mientras se da cumplimiento con los requisitos comerciales y otras obligaciones para protección de información.

3.5.1. Políticas Específicas

Esta sección describe las responsabilidades de dirección en seguridad de la información la aprobación de Política que cubren, El cumplimiento de la Política, la Educación del Usuario, la Seguridad del Sitio, Riesgos en la administración de la Información y Continuidad del Negocio, y los Acuerdos de Servicio con las Partes Externas.

3.5.2. Aprobación de la política

Política: El conjunto de políticas de seguridad de información se repasará periódicamente y aceptado de acuerdo a su pertinencia y relevancia de las prácticas comerciales, las partes responsables: los Miembros del departamento de Helpdesk aprueban las Políticas de Seguridad de Información. Estas políticas se someterán de manera rutinaria o de emergencia a actualizaciones para la administración de seguridad de la información de Omnes.

3.5.3. Cumplimiento de la política

Política: Cada unidad comercial llevará a cabo cada uno de las políticas de seguridad de información. Gerentes cuyas organizaciones no se adhieran a estas políticas, estarán sujeto a sanción disciplinaria por parte de la empresa.

Las partes responsables:

- Los gerentes comerciales supervisarán la aplicación , y reforzarán el cumplimiento de las políticas de Seguridad de Información, normas, y procedimientos, tanto para empleado y no empleados. (por ejemplo, contratistas, trabajadores a tiempo parcial, etc.).
- Administradores de Informática supervisarán el cumplimiento operacional de todos los sistemas, identificarán los riesgos de seguridad y sistemas no dóciles vía los procesos de QMS, y los funcionamientos correctos encontrados a ser no dóciles.

3.5.4. La educación del usuario.

Política: Cada usuario debe entrenarse en las prácticas de seguridad de información pertinente al uso de información de Omnes y sistemas. El entrenamiento debe estar fácilmente disponible y debe dirigirse a las necesidades básicas de cada tipo de obrero (es decir para Funcionarios de Seguridad de Sitio, el Administrador de red y sistemas de Informática, y los gerentes comerciales, ingenieros, etc.). Probando el conocimiento del usuario que deben ser mensurables y deben validarse a través de un programa de certificación.

Las partes responsables:

- El departamento de personal (Recursos humanos) es responsable para el entrenamiento en orientación de seguridad de todos los nuevos empleados en los principios básicos en seguridad de información.
- Los gerentes patrocinaran a los no empleados para su entrenamiento en orientación de seguridad.
- Los gerentes comerciales son responsables para informar a todos los empleados, a través de programas de conocimiento, sobre las políticas de seguridad de información, normas, y procedimientos. Los gerentes comerciales también son responsables para el entrenamiento y aprobación.
- Los Administradores de informática son responsables para el entrenamiento técnico para un trabajo específico del personal de informática designado.

3.5.5. La seguridad del sitio.

Política: A cada sitio se asignará un Funcionario de Seguridad de Sitio (SSO) y que prepara un documento de Procedimientos de seguridad del Sitio. El documento se dirigirá en todos los aspectos de la Norma de Seguridad de Sitio que se aplica al sitio y contendrá información suficiente que dirigirá los pasos razonables para proteger la pérdida de información confidencial de Omnes, dirigida a empleados, clientes, y vendedores, del acceso desautorizado, sobre la pérdida de integridad, y descubrimiento de información desautorizada. En el caso de un servicio de información, proteger su disponibilidad. Los procedimientos de Seguridad deben incluir el entrenamiento al usuario, su valoración, los informes del sistema de Dirección, y debe reimponerse rutinariamente para las posibles mejoras. Para los propósitos de seguridad del sitio, la red de información (SINet) será considerada un ambiente hostil, y el principio de menor privilegio será aplicado a todas las cuentas y acceso de la red.

Las partes Responsables:

- Los gerentes comerciales en cada situación seleccionan, entrenan, y apoyan un SSO.
- El SSO crea y mantiene el documento con los Procedimientos de Seguridad de Sitio y administra el programa de seguridad de sitio como una actividad de pérdida de control íntegro de las actividades de QHSE. SSOs también verifica la identidad del obrero y actúan como intermediario entre el resultado del incidente del obrero y el Equipo de respuestas a Incidentes de la corporación (IRT).
- QHSE es responsable para la creación y mantenimiento de una herramienta de reportes.

3.5.6. La administración de información y riesgos para la continuidad del negocio

Política: Deben realizarse la valoración de la Información y riesgos para la continuidad del negocio por cada sistema de informática y recurso usando procedimientos perfilados en las Políticas de administración de riesgos en seguridad de la información. Estas valoraciones deben realizarse con una frecuencia apropiada, dada la importancia del recurso.

Las partes responsables

- El administrador de Proyectos o diseñadores son responsables para el cumplimiento con todas las políticas, normas, y procedimientos hasta el lanzamiento de la producción.
- Los gerentes comerciales manejarán la información y los riesgos para la continuidad del negocio con los datos obtenidos del departamento de administración de riesgos, y los auditores de Informática.
- Debe proporcionarse un análisis de riesgos e inventario de información crítica y de los sistemas de negocio.

3.5.7. Los acuerdos de servicio con personas externas

Política: Los colegas comerciales de Omnes, contratistas, proveedores, clientes, y otros socios de negocio serán informados de sus responsabilidades de seguridad de información como parte de cualquier acuerdo de servicio o contrato. Todos los acuerdos de servicio especificarán un nivel apropiado de cumplimiento y responsabilidad para las pérdidas de seguridad. Cualquier acceso concedido a terceras personas será acorde con las condiciones del acuerdo de servicio y no debe permitirse más del acceso mínimo necesario para realizar el servicio. Las cuentas, el acceso físico a la información, y datos deben proporcionarse de una manera segura y removida o recuperada a la terminación del acuerdo de servicio. El Proveedor de servicios de medios externos debe ser auditado cada dos años. Se clasificarán datos y la propiedad intelectual apropiadamente y protegido durante el acuerdo, sin tener en cuenta qué medios se utilizan.

Las partes responsables

- El gerente patrocinador de cualquier acuerdo de servicio que requiera de conectividad de SINet es responsable para el cumplimiento con las políticas aplicables, normas, y procedimientos. Un gerente patrocinador también coordinará las cuentas de acceso los requisitos siguientes en ambas políticas de acceso a seguridad de Información y las políticas de Red en seguridad de la información.
- Los gerentes comerciales son responsables de administrar los riesgos de acuerdo de servicio.

3.6. POLÍTICAS Y PROCESO PARA LA ORGANIZACIÓN FÍSICA Y LÓGICA DE LA RED.

Los sistemas servidores de producción estarán en un cuarto físicamente seguro, con controles de acceso implementados de tal manera para que sólo personal autorizado tenga acceso a ellos. El administrador del sitio o el gerente de servicios de computación controlarán el acceso estrictamente a estos sistemas. La misma norma se aplicará a conectar equipos de telecomunicación a la red, como ruteadores, cortafuegos, y switches. Los sistemas de escritorio serán

físicamente asegurados a objetos inmóviles. Para computadoras portátiles desatendidas, deben ser físicamente aseguradas a objetos no portátiles (por ejemplo al escritorio, mesa, o puesto de trabajo) o puesto fuera de la vista en una área cerrada con llave (por ejemplo una oficina individual cerrada con llave, armario, o cuarto de conferencia). Se cerrarán con llave Oficinas donde estén localizadas computadoras desatendidas. Todos los sistemas tendrán instalado y activo los protectores de pantalla con contraseña. Si el sitio puede garantizar que hay un procedimiento de recuperación de todas las situaciones de emergencia (como pérdida de contraseña o de un empleado malévolo), todos los sistemas tendrán una de las siguientes contraseñas por lo menos habilitado:

- Una contraseña de arranque (una contraseña que debe ser ingresada antes que el sistema operativo arranque).
- Una contraseña de disco duro (una contraseña que desbloquee la información del sistema de archivos en el disco).

Se recomienda el desarrollo de un procedimiento corporativo para esta medida. En particular, una contraseña de arranque común es inadecuada para la seguridad. Para asegurar los datos en estos sistemas pueden recuperarse si es necesario, estas contraseñas deben ser depositados en un sitio seguro. Una alternativa es asegurar que la máquina sea respaldada correctamente al usar la solución de respaldos corporativa que asegura que esos datos puede recuperarse.

Todos los puertos servidos por el servidor DHCP se etiquetarán y se encontrarán en áreas de acceso controladas físicamente. En las redes mixtas (puertos DHCP y no DHCP).

3.6.1. Políticas para la seguridad de la información en Redes

Esta política describe la administración de dispositivos e interconexión de redes. Cubre las estructuras, métodos de transmisión, formatos de transporte, y medidas de seguridad usadas para las redes interiores y públicas. El cumplimiento con estas políticas asegura:

- El funcionamiento correcto y seguro de las facilidades de procesamiento de información,
- El riesgo minimizado del fracaso del sistema,
- integridad de software e información,
- La disponibilidad de procesamiento de información y comunicación,
- La prevención de daño en los recursos e interrupción en las actividades comerciales,
- La prevención de pérdida, modificación, o mal uso de intercambio de información entre las organizaciones.

Esta política se aplica a administradores de dispositivos de la red y máquinas que proporcionan servicios en la red. Los dispositivos de la red incluyen servidores, routers, bridge, concentradores, switch, firewalls, y las computadoras móviles. El conjunto de políticas de seguridad de información define las medidas requeridas para proteger los recursos de información para dar cumplimiento con los requisitos comerciales y otras obligaciones para protección de información.

3.6.2. Políticas Específicas

La red de información de Omnes o la Intranet está referida como SINet. Todos los usuarios de SINet que trabajan dentro de los medios de Omnes, usando información y sistemas, o conectado vía redes o acceso remoto obedecerán las condiciones de esta política. La falta de cumplimiento producirá la pérdida inmediata de todos los privilegios de acceso y otras consecuencias. El uso de cualquier recurso de Omnes o servicio de una manera impropia o no profesional acarreara una acción disciplinaria que puede incluir terminación del empleo del usuario o acuerdo de servicio. El incumplimiento será informado usando la herramienta de reportes de identificación de riesgos de la corporación (QUEST).

La Infraestructura de la red: Los siguiente puntos de la política se aplican a toda la infraestructura de la red y sistemas, sin tener en cuenta la función, incluso los routers, firewalls, servidores de Web, servidores de DNS, servidores de correo, servidores del Directorio Corporativos, y servidores de la base de datos.

- Todos los sistemas serán preparados y se manejarán según las normas de seguridad de sistemas. Esto incluye las normas de dirección de servicio para el correo, DNS, Web, y firwallls.
- Los Sistemas correrán sólo los servicios necesarios para realizar su función.
- Toda la infraestructura de la red y los sistemas se apoyarán para permitir la recuperación oportuna en caso de un fracaso.
- Se coleccionarán los archivos logs de Acceso en todo momento y protegido de sobreescritura accidental o deliberada.
- Los archivos logs incluirán los detalles de acceso por el usuario, actividades de reparación, intentos fallidos, y condiciones de error, como está descrito en las normas de seguridad de sistema pertinentes. Ellos deben grabar los cambios en los parámetros de login.
- Los archivos logs no deben detener los sistemas cuando los archivos logs lleguen a su tope.
- La responsabilidad e integridad de los archivos logs generados deben ser mantenidos.
- Se revisarán los archivos logs por lo menos mensualmente o como sea requerido según la situación del sistema.

3.6.3. Procesos de Seguridad para una Red

Cambio en la Administración Un cambio auditable en la administración de procesos se seguirá.

El Control de virus. Los servidores actuales de Correo incorporarán, facilidades de auto actualización y detección de virus.

El Mantenimiento remoto. El mantenimiento Remoto de la infraestructura de red de computadores será hecho usando los protocolos seguros. Para acceder a estos sistemas se concederá en una base de necesidad a uso. El acceso por conexión por línea conmutada a los servidores de la infraestructura o los dispositivos sólo se permitirá a través de servidores de acceso remoto certificados que se encuentran en la Norma de administración de ruteadores Cisco.

Las Contraseñas Las Contraseñas no pueden cruzar la red en texto claro.

3.6.3.1. Enclave Segura

Las aplicaciones de la Extranet se asegurarán mediante enclaves seguros y probados que siguen el Tercer punto del Procedimiento de Conexión. Las demandas para nuevas enclaves seguras seguirá el proceso de aprobación descrito en el Procedimiento de Conexión de Enclave Seguras.

El diseño de una Enclave segura será aprobado por el funcionario de diseño de SINet y el SSO. Se proporcionarán el plan actual y diagramas de la red al equipo de Seguridad de la SL-IT, al funcionario de diseño de SINet, y el Administrador de Seguridad de Recursos (RSM) responsables para la enclave. Cualquier cambio al plan de un enclave seguro requiere la aprobación de la Autoridad de diseño de SINet y el equipo de Seguridad de SL-IT. Lo siguientes puntos de las políticas definen el arreglo y el funcionamiento de un enclave seguro:

- Cada enclave seguro tendrá al menos un empleado de Omnes fijado como RSM. Si varios recursos diferentes se contienen en el enclave, es aceptable tener tantos RSMs como sean necesarios para rastrear toda la conexión y mantener las medidas de seguridad. Los RSMs deben tener un amplio y apropiado conocimiento técnico, comparable al papel del master en administración de sistemas.
- Los RSMs son responsables por cualquier brecha en seguridad de los sistemas de la Extranet e informarán vía el mecanismo de contestación de incidente corporativo.
- Los RSMs mantendrán un conjunto de procedimientos escritos de seguridad del Sitio de acuerdo con la Norma de Seguridad de Sitio y especificar a las funciones del enclave y los servicios que estas incluyen. El mantenimiento es la responsabilidad de los RSMs por los servicios en la enclave.

- Los servicios en un enclave seguro no puede tener el acceso a SINet. Cualquier excepción a esto requiere la aprobación específica de Seguridad de la SL-IT. El uso de protocolos seguros se requiere.
- La infraestructura de un enclave segura y servicios anotará las sesiones y eventos usando los medios especializados del Login.
- Una vez que un enclave para redes y servicios son activados, una auditoria periódica basada en sistemas críticos se realizará. Vea las Políticas en Administración en Seguridad de Riesgos de la información.
- Las conexiones de enclaves seguras se quitarán inmediatamente cuando por mucho tiempo no se hayan requerido.
- Las conexiones realizadas por propósitos administrativos usarán protocolos seguros.
- Los Servicios que residen en enclaves seguras adherirán las siguiente reglas:
  - El servicio será configurado y se mantendrá según las normas del sistema de Omnes, como mínimo.
  - El servicio tendrá un plan documentado de administración de seguridad dentro del enclave los Procedimientos de Seguridad de Sitio.
  - El servicio sufrirá una auditoria de seguridad por lo menos cada seis meses.

3.6.3.2. Las Conexiones directas desde SINet a las Redes que no pertenecen a SINet

Los métodos aceptados para conectar SINet a las redes externas son limitadas para los Gateways de Internet, los dispositivos proxy, y enclaves seguros aprobados ó administradores de firewalls. Todas las excepciones a estos métodos deben ser aprobadas específicamente por el equipo de Seguridad de SL-IT. Los dispositivos involucrados en estas conexiones se adherirán a las siguientes reglas:

- **Los Routers** estarán al frente en redes que no sean de SINet administrando de manera centralizada y segura de acuerdo a la lista de

control de instalación de Routers seguros. El equipo de seguridad de SL-IT debe aprobar todas las variaciones a la norma para esta clase de Routers.

- **Web Proxies y Caches** Los proxies Web en los que está basado SINet que enfrentan a las redes que no son de SINet con conexiones directas a la Internet se manejará y logoneará centralmente según la Norma de servicios Proxy/Cache. Otros Web proxies y caches reunirán los requisitos actuales mínimos en requerimientos de diseño de SINet. El equipo de seguridad SL-IT debe aprobar todas las nuevas instalaciones y cambios a los procesos aceptados.
- **Gateways, Enclaves Seguras, Firewalls** Los Gateways, enclaves seguras, y firewalls serán centralmente administrados y fogoneados de acuerdo a los procedimientos aprobados por SL-IT. El equipo de seguridad de SL-IT debe revisar y aprobar todas las nuevas instalaciones y cambios a procesos aprobados.

Se prohíben las conexiones de red estrictamente, incluso la conexión por línea conmutada directamente de los hosts de SINet a redes de datos externas o a un grupo de computadores conectados. No se conectarán máquinas usadas para este propósito a SINet. El acceso de SINet a la Internet está generalmente abierto, con sólo unas excepciones. Estas excepciones se manejan por el equipo de Seguridad de SL-IT y son sujetos al cambio a su discreción. Las excepciones son hechos basados en el nivel de riesgo.

3.6.3.3. Las Conexiones directas de Redes Externas a SINet

- **Los Firewalls.** Todas las conexiones procedentes de redes externas terminarán en una enclave seguro aprobada por SL-IT. El acceso directo de la Internet a SINet puede ser permitido por ciertas aplicaciones, hosts, o protocolos después de la aprobación específica hecha por el equipo de Seguridad de SL-IT y sólo en una temporada, según la base caso por caso.
- **Acceso remoto**. Todo acceso a SINet por medio de redes externas o de máquinas individuales será a través en una Red privada Virtual aceptada (VPN), portal de acceso, o un servidor de acceso certificado. La tecnología de acceso remoto está cambiando rápidamente, de tal manera

que otros métodos deben ser calificados. Sin embargo todos los métodos de acceso remoto y tecnología deben ser aprobadas específicamente por el grupo de Seguridad de la SL-IT.

- **Las Conexiones de red.** Las conexiones de red que no usan un método de acceso remoto aceptado estrictamente están prohibidas. Esto incluye la conexión por línea conmutada directamente a redes de Omnes o los hosts de las redes de datos externas, hosts de redes de datos externas, o hosts individuales.

3.6.4. La Manera apropiada de Supervisar la Red

El éxito comercial depende del apropiado y seguro funcionamiento de la red de computadores. Por consiguiente se supervisan las actividades de la red para posibles violaciones de seguridad o el uso inapropiado, incluso de ataques externos. Sin embargo, la información personal sobre los empleados de Omnes también se guarda y es transmitida en la red. Desde los valores de jubilación de los trabajadores de Omnes, la información personal debe ser protegida de accesos desautorizados o la exposición impropia para monitoreos de la red. En general, la información personal de un empleado sólo debe examinarse por los monitoreadores de la red como un requisito de la dirección para una administración apropiada de los medios de IT y para futuros negocios de la compañía.

- Las herramientas de monitoreo (Intermapper) de la red debería ser utilizada solo por razones legítimas de seguridad de la red.
- Las herramientas de monitoreo de la red deberían ser configuradas para recoger información que ha sido revisada por un operador humano y sólo por razones legítimas de negocio o como dirigido para las agencias de ejecución de la ley. Siempre sea posible, la recolección de datos debe ser realizado por el software y hardware y debe protegerse automáticamente para evitar un mal uso o brechas de seguridad.
- Las herramientas de monitoreo de la red deberían ser usadas por personal especializado y autorizado como parte de su definición de las funciones

(por ejemplo, por especialista de seguridad de IT o el miembro de Equipo de respuestas a Incidentes).

- Las herramientas de monitoreo de la red deberían ser protegidas físicamente y electrónicamente y físicamente del acceso desautorizado.

La Investigación de incidentes

- Investigar rápidamente los incidentes con el respeto debido para el retiro de los individuos identificados.
- Examinar las actividades de empleados específicos solo si hay evidencia satisfactoria que los implica en un incidente real.
- Durante la investigación, proteger contra el descubrimiento innecesario o desproporcionado de información personal.
- Evitar un examen o descubrimiento de información delicada como racial o origen étnico, opiniones políticas, religioso o creencias filosóficas, afiliación sindical, e información que relacionan a salud o sexo.
- La información que se recolecto en el curso de una investigación estarán al tanto de ella los departamentos de Personal (Recursos humanos), gerentes, departamentos legales e involucrados en la investigación.
- Use monitoreo de contenido en tiempo real de comunicaciones del empleado sólo cuando 1) hay razón para creer que el individuo puede haber violado política de uso de red o haberse comprometido con la seguridad de la red, 2) otras, cuando las medidas de detección de intrusos no han sido efectivas para proteger la red, 3) cuando monitorear es aceptado por el departamento legal de Omnes.
- Los datos recogidos y guardados como parte de una investigación debe ser electrónicamente y físicamente protegidos del acceso desautorizado.

El descubrimiento

- No descubrir información personal obtenida durante el monitoreo de la red a personas ajenas a la compañía a menos que hay el consentimiento del departamento legal de Omnes.

- El descubrimiento interior de información personal obtenido durante el monitoreo de la red sólo debe hacerse como parte de protección de seguridad de la red y en un base de necesidad de conocer. En general se limita a miembros del departamento Legal, Personal, y gerentes involucrados en dirigir una violación de seguridad.
- Información anecdótica usada para fortalecer el conocimiento debe sanearse para prevenir la identificación de terceras personas.

3.6.5. La Administración de la política

- El Funcionario jefe de Información de Omnes es asignado la responsabilidad global para procesar la información.
- Cada Unidad Comercial es responsable en rastrear y publicar en el Web interior una lista de enclave internas y externas, todos los servicios expuestos externamente, y RSMs asociados.
- Los RSMs son responsables para aprobar los nuevos servicios en un enclave seguro y agregando a los nuevos clientes a un enclave seguro.
- Los RSMs son responsables para administrar la seguridad de sus recursos asignados en un enclave.
- Los Administradores del Sistema son responsables para la instalación, la configuración del host, el control de acceso, los archivos logs de acceso, y protección de virus en toda la red de área local (LAN) los servidores y las computadoras personales conectadas a la red (PCs).
- Los Administradores del Sistema, departamento de operaciones, los de helpdesk, Funcionarios de Seguridad de Sitio, y los miembros de Equipo de respuesta a Incidentes son responsables para el funcionamiento diario, dirección en incidentes, cambios de administración, monitoreo del sistema, y continuidad del servicio.

3.7. POLÍTICAS EN ADMINISTRACIÓN DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN

La información y los sistemas en que estos residan son vitales para el negocio de Omnes. Los dos requieren protección en proporción por su valor comercial.

El objetivo de esta política es asegurar que los planes existan para identificar los recursos de información comercial críticos y las amenazas a esos recursos, e identificar y utilizar los resguardos rentables para mitigar los riesgos.

El conjunto de políticas de seguridad de información define las medidas requeridas para proteger los recursos de información mientras se da cumplimiento con los requisitos comerciales y otras obligaciones para protección de la información.

3.7.1. Políticas específicas

Los gerentes Comerciales son responsables para la valoración apropiada y mitigación de riesgos de los sistemas y la información en sus organizaciones respectivas.

Identificación de los Sistemas críticos

Un inventario de sistemas que contienen datos críticos o se realizan procesos de negocio críticos sea mantenido o referenciado en un documento de Procedimientos de Seguridad del Sitio. Este inventario debe ponerse al día de acuerdo a los sistemas que se agregan y debe ser revisado anualmente.

Un sistema está definido como crítico cuando el impacto comercial asociado con la pérdida o compromiso de uno o más conjuntos de datos o procesos de negocio exceden el nivel de pérdida de “Mayor”. Los costos incluyen reemplazo del sistema, el reemplazo del software, la recuperación de datos, la pérdida de la situación estable, y pérdida de negocios actuales o futuros.

Los Sistemas para inventariar incluyen pero no se limitan a routers, servidores, estaciones de trabajo, sistemas de ayuda, y sistemas de comunicación.

Valoración de Riesgos

Una valoración de riesgos que utiliza la Norma de Valoración de Riesgo en Seguridad de la Información será realizada en la lista de sistemas críticos para

identificar las amenazas contra la información, sistemas, y procesos. Se realizarán los posibles escenarios de fracaso y estimaciones de impacto para cada sistema crítico. Cada escenario debe identificar que proceso comercial requiere protección.

Plan de Mitigación de Riesgos

Un Plan de Mitigación de Riesgo se escribirá para reducir los riesgos de la información y de los sistemas a un nivel manejable, adecuado para la administración comercial. Los costos y beneficios de resguardos potenciales serán revisados, y se pondrán los resguardos rentables en el lugar para mitigar los riesgos identificados. Además de la aplicación apropiada de medidas de tecnología, el plan incluirá:

- La lista de personas responsables y alternantes, según las tareas claves.
- Los procedimientos para reasumir el procesamiento de la información que sigue a un incidente, incluso el entrenamiento aplicable al usuario. Los planes serán distribuidos, de acuerdo al nombre de la tarea, a las personas requeridas para restaurar la información, sistemas, o servicio en una emergencia. Los procedimientos deben escribirse para que aquéllos que normalmente no los llevan a cabo, puedan hacerlo.
- Las especificaciones para cuándo invocar el plan, el tiempo estimado para la restauración de servicios, y horario de tareas. Se listarán los procedimientos de recuperación en el orden en que ellos serán realizados.
- Procedimiento para procesar atrasos construidos durante el paro del sistema o cómo reasumir el proceso que usan los medios alternativos.
- El procedimiento para restaurar los servicios, incluso el teléfono, la comunicación de datos, el personal, construcción de accesos, electricidad, y agua.
- Los medios alternativos para organizar las aplicaciones críticas.
- Un adecuado fondo de seguro en seguridad de información. El seguro debe dirigirse a pérdida de datos, interrupción comercial, y obligaciones a

terceras personas. Debe proporcionar protección adecuada contra fuego, robo, fraude, o el daño malévolo.

- Los aspectos legales y contingencias.
- Los sistemas críticos serán apoyados por medidas de protección y seguridad aplicadas en relación al valor de la información o procesos.

3.7.2. Políticas para el almacenamiento y reciclado de cintas

Objetivo.- Definir las pautas que se deben seguir para recuperar la información y lo más importante la protección de la misma.

Responsable: Ing. Santiago Jaramillo

Políticas: El proceso de Almacenamiento y Reciclado de cintas seguirá las siguientes políticas encaminadas a resguardar la información contenida en las mismas:

- Se utilizara como único sistema de realización de respaldos el sistema Backup Exec.
- Las cintas incrementales se podrán reciclar una vez que hayan cumplido 30 días de antigüedad.
- Las cintas Totales se podrán reciclar una vez que hayan cumplido 45 días de antigüedad.
- Las cintas Totales que coincidan con el fin de mes, considerando fin de mes las fechas incluidas entre el 25 de un mes y el 5 del mes siguiente, no se reciclarán.
- Las cintas serán guardadas en la caja fuerte de la gerencia, considerado el sitio más seguro de las oficinas.
- Se enviarán mensualmente a un servicio de almacenamiento bancario las cintas que tengan por lo menos 60 días de antigüedad
- Será solicitado mensualmente que se traigan las cintas del almacenamiento bancario con el fin de escoger las cintas para reciclado y enviar las que hayan cumplido los 60 días o sean cintas de fin de mes.

- La persona responsable de los traslados de las cintas entre la oficina y el servicio de almacenamiento externo será un mensajero asignado para el fin por OFS y será responsabilidad de OFS cualquier accidente o pérdida durante este traslado.

3.8. EQUIPOS Y PROCEDIMIENTOS DE EMERGENCIA EN CASO DE UNA CONTINGENCIA

En esta etapa se definen los procedimientos de emergencia y recuperación, así como los equipos que los ejecutarán y los integrantes de estos equipos. A continuación se describen las tareas que la componen.

3.8.1. Definición de los equipos de contingencia.

Las acciones que se deben tomar para efectuar el establecimiento de un desastre, son llevadas a cabo por equipos de recuperación, cada uno con su propia responsabilidad.

Al realizar esta tarea, debemos recordar que estamos planeando para el peor de los casos, la destrucción total de la instalación del centro de cómputo; también hay que considerar que la definición de los equipos y de su membresía, es decir, las áreas que estarán representadas en el equipo, así como de sus funciones especificas durante la recuperación del desastre.

Obviamente se deben adaptar los equipos a las circunstancias existentes, dependiendo de factores tales como número, tamaño y sofisticación del centro de cómputo e importancia de la función de sistemas “Helpdesk” en la empresa.

3.8.2. Coordinador del Plan de Contingencia.

Sus funciones son las siguientes:

- Decidir si se declara la contingencia o no, si únicamente se establecen medidas temporales de seguridad.

- Vigilar que el plan permanezca actualizado y adecuado (actualizado, mantenimiento y pruebas).
- Se encarga de la administración y el manejo del presupuesto que se ejerza durante la puesta en marcha del plan.
- Vigilar que la instalación de respaldo seleccionada se mantenga con las condiciones necesarias para cumplir las especificaciones.

3.8.3. Subcoordinador del Plan de Contingencia

Sus funciones son las siguientes:

- Obtener las provisiones y servicios generales (p. eje., transporte de personas y equipo) necesarios durante la contingencia hasta el restablecimiento de operaciones normales
- Autorizar y vigilar el acceso a la caja de seguridad externa.
- Mantener el contenido e inventario de la caja de seguridad actualizado y completo. La decisión de alguna nueva inclusión o exclusión será en conjunto con el Coordinador.

3.8.4. Equipo de Comunicaciones

Sus funciones son las siguientes:

- Dotar de todas las comunicaciones y telecomunicaciones necesarias (en la medida de lo posible) a la instalación de respaldo, tratando de evitar la discontinuidad en el funcionamiento de los sistemas a causa de problemas en las telecomunicaciones entre la instalación de respaldo y las entidades con las que normalmente tiene comunicación frecuente la empresa. A este aspecto, la telefonía celular debe considerarse como posible respaldo para comunicaciones, para lo cual hay que tomar en cuenta lo siguiente los teléfonos de mano operan a 0.6 Watts, en este caso de desastre algunas células de la red podrían salir de funcionamiento por lo que se requiere comunicarse con otras células mas lejanas; en este caso requerirá la potencia adicional de un teléfono “trasportable” de 3 Watts, otro limitante

que hay que prever de los teléfonos celulares la duración de sus baterías, se requerirán teléfonos con baterías de mayor duración, también pueden adquirirse baterías adicionales, y mantenerlas cargadas permanentemente. Si en el área hay más de una compañía que da el servicio de telefonía celular, podrían obtenerse teléfonos que permitan "registro dual de números" para funcionar con los dos sistemas. En esa forma, si una red se cae o se congestiona usted puede cambiar a la otra. Otra característica que puede ser útil es la memoria alfanumérica. Los nombres y números de se almacenan electrónicamente; esto elimina la necesidad de una lista de teléfonos que puede perderse en el desastre. Independientemente de qué teléfono se seleccione, asegúrese de que las personas sepan usarlo. Además, hay que probar los teléfonos celulares cada dos o tres meses para verificar que funcionan adecuadamente. Los teléfonos celulares deberían comprarse antes que ocurra un desastre. No sólo estarán disponibles cuando se necesiten sino que los números puede ser dados a conocer al personal de los equipos de recuperación para que reciban las llamadas de las personas que tendrán que comunicarse con ellos.

- Realizar todo lo necesario para instalar la infraestructura de comunicaciones en el nuevo centro de procesamiento de datos o reinstalar en el centro de reparación.

3.8.5. Equipo de representantes de Usuarios.

Sus funciones son las siguientes:

- Comunicar a sus respectivas áreas los procedimientos de operación durante la contingencia, restricciones, procesos especiales, etc. Además debe supervisar quienes son las personas de sus respectivas áreas que van a trabajar en la instalación de respaldo.
- Ver que el lugar en la instalación de respaldo, en donde llegarán los usuarios a trabajar, cuenten con todo lo necesario.
- Ellos constituirán el puente entre la instalación de respaldo y el local donde se encuentre la empresa.

- En el caso de un desastre natural de alcance regional, los directores de cada área deben comunicar los problemas que tuviera estas personas al equipo de apoyo al personal o al coordinador del plan de Contingencia.

3.8.6. Equipo Evaluador

Sus funciones son las siguientes:

- Debe evaluar el daño al centro de cómputo y en general a todo el equipo y redes de cómputo con que cuente la empresa, así como el daño a los sistemas, a la información, etc. Para esto, debe servirse del inventario que se realizo previamente. También es su deber rescatar lo que aún puede servir.

3.8.7. Equipo de Organización y Operación de la Instalación de Respaldo.

Sus funciones son las siguientes:

- Llevar toda la información (cintas o discos) pertinente, de acuerdo con lo establecido en el plan de contingencia y a las indicaciones del coordinador del plan.
- Llevar e instalar todo el software y hardware necesario para que puedan procesar los sistemas críticos.
- Operar el sistema y llevar a cabo todos los procesos necesarios (producción y respaldos) de acuerdo con el plan de contingencia. Deben poner especial énfasis en la seguridad y el acceso a los sistemas de la organización.

3.8.8. Equipo de Recuperación de Instalaciones.

Sus funciones son las siguientes:

- Con base en el inventario y en el diagnóstico del equipo de evaluación, deberá concentrarse en la reconstrucción de todas las instalaciones de

cómputo, obedeciendo las indicaciones del Coordinador del Plan, que es la persona que está en contacto con la Alta Dirección de la Empresa.

- También debe asegurar la disponibilidad de hardware necesario en la instalación de respaldo (si hiciera falta algo en el momento). Esta tarea la realiza en forma conjunta con el equipo de organización y operación de la instalación de respaldo.

3.8.9. Equipo de Apoyo al Personal

Finalmente, se considera la creación de otro equipo que, aunque no es propiamente "operativo" del plan de contingencia, es posiblemente el más importante, ya que si no actúa en forma eficiente y expedita, todo el plan de contingencia podría verse paralizado por falta de personal que lo ejecute.

Sus funciones son las siguientes:

- Prever asistencia y primeros auxilios al personal herido.
- Alertar a los servicios médicos para que concurran en auxilio del personal afectado.
- Debe prever apoyo para los requerimientos personales de los empleados.
- Se debe tratar de resolver cualquier necesidad de la familia del empleado.

3.9. Conformación de los Equipos.

Conformar los equipos ha requerido de la identificación del personal que tiene habilidades y conocimientos necesarios para desempeñar las tareas que les son designadas. Hay que tener en cuenta que debido a que cada equipo tiene su función, sus miembros sólo necesitan la capacidad para realizar los procedimientos correspondientes a sus funciones los equipos quedaron conformados de la siguiente manera:

Coordinador del Plan de Contingencias: Jefe de Proyectos Especiales:
Fabiola Vejarano
Suplente: Jefe de Proyectos

Santiago Jaramillo

Subcoordinador del Plan de Contingencias: Jefe de Proyectos
Santiago Jaramillo
Suplente: Wilson Suárez.

Equipo de Comunicaciones

Coordinador**:** Funcionario de Seguridad de Sitio (SSO):
Wilson Suárez.
Suplente: Operador del departamento de Helpdesk
Gabriel Eguiguren.
Miembros:
Ejecutivo de Ventas: Wladimir Luna
Ejecutivo de Ventas: Alfredo Shulca.

Equipo de representantes de los Usuarios

Coordinador: Operador del departamento de Helpdesk
Ximena de la Vega.
Suplente: Operador del departamento de Helpdesk
Paulina Sánchez
Miembros:
Mónica Aviles
Liset Acuña.

Equipo de organización y operación de la instalación de respaldo

Coordinador: Jefe del departamento de Mercadeo:
Melino Ramos
Suplente: Operador del Centro de Cómputo:
Paulina Sánchez
Miembros:
Operador del centro de cómputo: Paulina Sánchez.
Operador del centro de cómputo: Ximena de la Vega

Equipo de Recuperación de Instalaciones

Coordinador: Gerente

Amparo MENA

Suplente: Jefe Administrativo

María Mercedes Carrera.

Miembros:

Lisett Acuña

Eliana Quiroz.

Equipo de Apoyo al Personal

Coordinador: Asistente de Recursos Humanos

Mónica Aviles

3.10. IMPLEMENTACION DEL PLAN DE CONTINGENCIA

3.10.1. PLAN DE CONTENCIÓN

En el plan de contención se establecen todas aquellas acciones que se deben tomar cuando se esta presentando un problema; es decir, este plan detalla “como enfrentar lo que ocurra en la compañía”. Para el tratamiento de los problemas que se pueden presentar en la empresa, se elaborará una bitácora de atención para cada tipo de problema, el mismo que se actualizará cuando la empresa esté afrontando un determinado problema.

La bitácora contendrá la siguiente información:

- Fecha del problema.
- Usuario que reporta el problema.
- Tipo de problema.
- Infraestructura física.
- Hardware.
- Software.
- Respaldos.

- Comunicaciones.
- Detalle del Problema.
- Técnico o área que atiende el problema.
- Estado de la bitácora.
- Asignado (cuando el HelpDesk esta notificado del problema).
- Cerrado (cuando el problema esta resuelto).
- Solución del problema.

La bitácora permitirá al departamento de HelpDesk llevar un control de los problemas que pueden suscitarse, siendo lo más importante el que permitirá enfrentar de mejor manera los problemas que ya se suscitaron anteriormente, ya que se tiene una referencia de la solución que se realizó a dicho problema.

Evaluación de los Daños

Se lo realiza para determinar cuales son los sistemas que fueron afectados por el desastre, determinando a su vez cuales han quedado no operativos, cuales se pueden recuperar y el tiempo que se necesita para éste proceso.

La evaluación de los daños también nos determinará si la compañía afronta un problema de corta duración o un desastre de larga duración.

Problemas de corta duración

Denominaremos problemas a aquellos inconvenientes que tienen un efecto de corta duración, es decir, la empresa no requiere poner en marcha el plan de supervivencia para afrontar el problema.

Cabe indicar que se puede presentar un mismo problema con un nivel de efecto diferente, en donde, de acuerdo a su efecto se pondrá en marcha el plan de supervivencia según sea el caso. Por lo tanto se encuentra mencionado aquellos problemas que pueden tener un efecto de larga duración, los que requerirán la ejecución del plan de supervivencia y su plan de contención se encuentra descrito posteriormente en el tema “Desastres de larga duración”.

los problemas más comunes que se pueden presentar en la compañía son los siguientes:

Infraestructura Física

Terremoto, Incendios

- Evacuar al personal y clientes de Omnes, que se encuentren ese instante en el edificio por las escaleras.
- Utilizar aquellos extintores de mayor accesibilidad.
- Realizar las llamadas pertinentes a:

  Bomberos 102
  Policía Nacional 101
  Cruz Roja 131

- Notificar a la gerencia de los posibles daños.
- Si es el caso activar el plan alterno en Colombia (Plan de Supervivencia)

Falla en la Planta de Energía

Diagnóstico: Cuando la planta no se active automáticamente o manualmente en el momento de pérdida de suministro de energía por parte de la empresa eléctrica.

- Notificar al Jefe se Sistemas y al Administrador del edificio.
- Actualizar la bitácora de atención de problemas para la administración del edificio.
- Informar a los usuarios el daño e indicar que los UPS disponen de 15 a 20 minutos de energía eléctrica, para poder salvar su información y apagar el equipo normalmente.
- Realizar el seguimiento de la resolución del problema a la administración del edificio.

Daño del Sistema eléctrico

Diagnóstico: Cuando no se tiene energía eléctrica en un área específica del edificio, o en una toma corriente determinada.

- Notificar al Jefe de Sistemas y al Administrador del edificio.
- Actualizar la bitácora de atención de problemas para la administración del edificio.
- Desconectar los breakers correspondientes al área con problemas.
- Desconectar los equipos de los enchufes eléctricos.
- Revisar la posible causa: corto circuito, sobre voltaje o mala instalación eléctrica.
- Realizar el seguimiento de la resolución del problema a la administración del edificio.

Fallas de la red UPS (Alternativa 1)

Diagnóstico: Cuando no se tiene energía eléctrica en las tomas de UPS, en los momentos de falla de suministro de energía eléctrica.

- Notificar al Jefe se Sistemas del problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Desconectar los equipos de las tomas de UPS
- Activar los UPS individuales de aquellos equipos críticos como servidores y computadoras personales de importancia.
- Llamar a la empresa proveedora de la red de UPS para que solucione el problema.
- Realizar el seguimiento de la resolución del problema a la empresa proveedora de la red de UPS.

Fallas en los UPS (Alternativa 2)

Diagnóstico: Cuando no se tiene energía eléctrica en el UPS, en el momento que se desconecta el mismo de la toma eléctrica.

- Notificar al Jefe se Sistemas del problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Desconectar los equipos de las tomas de UPS individual.
- Llamar a la empresa proveedora del UPS para que solucione el problema.
- Realizar el seguimiento de la resolución del problema a la empresa proveedora del UPS.

Hardware

Problemas con los dos Servidores

Caso: En el caso de que el desastre afecte en su totalidad el funcionamiento del Servidor Central y el de Backup, se debe poner en marcha la activación del plan alterno (Plan de Supervivencia).

Problemas de uno de los Servidores

Caso: Cuando el servidor deja de funcionar correctamente por problemas en los dispositivos o por falla de la fuente de alimentación

Falla del Servidor Backup

- Notificar al Jefe se Sistemas del problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Determinar si el daño es en algún dispositivo del Servidor o en la fuente de alimentación.
- Referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a la empresa contratada para el mantenimiento preventivo correctivo para que repare la falla del Servidor Backup.
- Desactivar el Servidor Backup.
- Realizar el seguimiento de la resolución del problema a la empresa contratada para mantenimiento.

Falla del Servidor Central

- Notificar al Jefe se Sistemas del problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Determinar si el daño es en algún dispositivo del Servidor o en la fuente de alimentación.
- Activar el Servidor Backup como principal.
- Verificar que el Servidor Backup esté operando correctamente por medio del sistema de monitoreo.
- Realizar el seguimiento de la resolución del problema a la empresa contratada para mantenimiento.

Daño en los discos duros de las estaciones

Diagnóstico: Cuando no reconoce el disco duro, o no se puede acceder al mismo.

- Notificar al Departamento de HelpDesk y Soporte al Cliente lo ocurrido y cual es la estación que tiene el problema.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Revisar el equipo y comprobar si el daño es lógico o físico del disco duro.
- Llamar a la empresa proveedora, si el daño es físico y requiere el cambio de disco duro.
- Realizar el seguimiento del cambio de disco duro a la empresa proveedora.
- Si es el caso y dependiendo del tipo de usuario, utilizar un equipo de respaldo de acuerdo a la tabla 2-18

Error en la memoria RAM de las estaciones

Diagnóstico: Cuando se cuelga el computador desplegando una pantalla azul con error de memoria al ejecutar alguna aplicación o al iniciar Windows.

- Notificar al Departamento de HelpDesk y Soporte al Cliente lo ocurrido y cual es la estación que tiene el problema.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Llamar a la empresa proveedora para que den solución al problema.
- Realizar el seguimiento del cambio de memoria a la empresa proveedora.
- Si es el caso y dependiendo del tipo de usuario, utilizar un equipo de respaldo de acuerdo a la tabla 2-18

Daños en las tarjetas controladoras de las Estaciones

Diagnóstico: Cuando los mensajes de error no indican problemas en los archivos de sistema o en los controladores de las tarjetas.

- Notificar al Departamento de HelpDesk y Soporte al Cliente lo ocurrido y cual es la estación que tiene el problema.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Llamar a la empresa proveedora para que den solución al problema.
- Realizar el seguimiento del cambio de la tarjeta controladora a la empresa proveedora.
- Si es el caso y dependiendo del tipo de usuario, utilizar un equipo de respaldo de acuerdo a la tabla 2-18

Pérdida o daños graves de las laptops

Diagnóstico: Cuando el cambio de la laptops es irremediable.

- Notificar al Departamento de HelpDesk y Soporte al Cliente de lo ocurrido.
- Comprobar la pérdida o daño de la laptop.
- Justificar el cambio de la laptop.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Llamar a la empresa proveedora para realizar el cambio del equipo.

- Realizar el seguimiento cambio de laptop a la empresa proveedora.

Software

BASE DE DATOS

Problemas de acceso a la base de datos del SafiWin en el Servidor Central

Diagnóstico: Cuando no se puede acceder a la base de datos del SafiWin a pesar de que la base de datos se encuentra alzada en el Servidor Central y que la estación cliente del SafiWin se encuentre en red.

- Notificar al Jefe se Sistemas de lo ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Informar a los usuarios del SafiWin el problema del mismo.
- Llamar a la empresa proveedora del sistema SafiWin para que den solución al problema y pueda ser resuelto lo antes posible.
- Realizar el seguimiento de la solución al problema a la empresa proveedora.

Problemas de acceso a la base de datos del SAP Basis

Diagnóstico: Cuando no se puede acceder a la base de datos del SAPBasis a pesar de que existe comunicación con el Servidor en Houston y que la estación cliente del SAP Basis se encuentre en red.

- Notificar al Jefe se Sistemas de lo ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Informar a los usuario del SAP Basis el problema del mismo.
- Llamar al HelpDesk de Schlumberger en Houston para que den solución al problema y pueda ser resuelto lo antes posible.

- Realizar el seguimiento de la solución al problema al HelpDesk en Houston.

SERVIDORES

Problemas de sistema en el Servidor Central

Diagnóstico: Cuando el Servidor no arranca correctamente, no se alzan correctamente los servicios y los mensajes de error no son de los dispositivos del Servidor.

- Notificar al Jefe de Sistemas el problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Apagar el servidor.
- Activar el servidor de respaldo para que continúe normalmente las operaciones de Omnes.
- Verificar que el Servidor Backup levante todos los servicios y esté operando correctamente.
- Verificar que exista comunicación nuevamente.
- Revisar el daño y determinar si se necesita la presencia de la empresa proveedora del Servidor, o si se hace cargo el departamento de HelpDesk y Soporte al Cliente.
- Analizar el porque del problema ocurrido.
- Realizar el seguimiento de la solución al problema.

Perdida o daño de archivos del Servidor de datos

- Notificar al departamento de HelpDesk y Soporte al Cliente.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Determinar con el usuario la última fecha que trabajo con esa información correctamente.
- Identificar el cartucho de acuerdo a la fecha.

- Recuperar y copiar el archivo.
- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

Procesos inhibidos en el Servidor de Comunicaciones (Windows NT)

Diagnóstico: Cuando por instancias no determinadas el Servidor deja de trabajar, perdiendo los servicios de la red.

- Notificar al Jefe de Sistemas el problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Bajar el Servidor.
- Revisar que proceso fue el causante del problema de comunicación.
- Subir el Servidor nuevamente.
- Verificar que exista comunicación nuevamente a través del sistema de monitoreo.
- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

ESTACIONES

Daño en los archivos de sistema de las estaciones Diagnóstico: Cuando Windows no inicia correctamente.

- Notificar al Jefe de Sistemas el problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Iniciar Windows en modo prueba de fallos.
- Realizar un scandisk para reparar los archivos de sistema que se encuentren dañados, y si es el caso verificar que se marquen los sectores dañados para que estos no sean utilizados una próxima vez.
- Analizar el porque del problema ocurrido.

- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

Daño en los archivos de aplicaciones de las estaciones

Diagnóstico: Cuando la aplicación no se inicia correctamente.

- Notificar al Jefe de Sistemas el problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Determinar que aplicación tiene el problema y la versión de la misma.
- Determinar que archivos son los dañados y en que path se encuentran.
- Reemplazar los archivos dañados por otros archivos copiados de un computador que tenga instalado la misma versión de la aplicación y que esté trabajando correctamente.
- Analizar si se debe reinstalar la aplicación que tiene problemas.
- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

Caso de Virus

- Notificar al departamento de HelpDesk y Soporte al Cliente cual es la estación que se encuentra infectada por el virus.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Reiniciar el equipo con un disquete de arranque, preferible con el disquete de emergencia que lo genera el antivirus.
- Ejecutar el antivirus.
- Eliminar el virus encontrado.
- Si es el caso, borrar el archivo si en éste no ha sido eliminado el virus, y restaurar el mismo del respaldo más reciente.
- Reiniciar el equipo.

- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

Respaldos

- Falta de espacio en el Servidor de datos
- Notificar al Jefe de Sistemas del problema ocurrido.
- Actualizar la bitácora de atención de problemas al Administrador de la red.
- Reparar el disco duro de backup. Insertar el disco duro en uno de los slots disponibles del Servidor de Datos, sin necesidad de Apagar el Servidor. El Servidor detectará éste automáticamente (en caliente).
- Verificar el aumento de espacio en el Servidor de Datos.
- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

Incumplimiento de la obtención de los respaldos

- Notificar al Jefe de Sistemas del incumplimiento de la obtención de respaldos.
- Establecer la sanción pertinente.
- Actualizar la bitácora de atención de problemas al Administrador de la red.
- Realizar la obtención de los respaldos inmediatamente.
- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

Comunicaciones

Pérdida de Comunicación con el Servidor

- Notificar al HelpDesk del problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Revisar el daño y determinar el caso de que ningún usuario tiene comunicación con el Servidor

- Activar el Servidor de Backup
- Verificar que el Servidor esté operando correctamente por medio del Sistema de monitoreo.
- Analizar porque no se tiene comunicación con el Servidor Principal.
- Cuando un área no tiene comunicación con el Servidor
- Referirse a la garantía del hub correspondiente al área con problemas si este se encuentra dentro del periodo del mismo, caso contrario, contactar a la empresa proveedora para reemplazar el hub por otra igual o de similar característica.
- Cuando una estación no tiene comunicación con el Servidor
- Referirse a la garantía del equipo si este se encuentra dentro del periodo del mismo, caso contrario, informar a la empresa contratada para mantenimiento, para reemplazar la tarjeta de red por otra igual o de similar característica.
- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

Fallas en la Central Telefónica

- Notificar al HelpDesk del problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk
- Revisar el daño y determinar si se necesita la presencia de la empresa proveedora de la Central Telefónica, o si se hace cargo el departamento de HelpDesk y Soporte al Cliente.
- Analizar el porque del problema ocurrido.
- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

Desconectarse de la comunicación a través de la intranet mundial de Schlumberger “SINet”

- Notificar al HelpDesk del problema ocurrido.

- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Revisar y determinar si el problema es en alguno de los dos router Cisco, si lo es resolverlo lo más pronto posible.
- Si es el caso, llamar al proveedor de comunicaciones (Impsat), si el daño es en la antena o en el tele puerto.
- Analizar el porque del problema ocurrido.
- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

Desactivación de la comunicación solo a Internet

- Notificar al HelpDesk del problema ocurrido.
- Actualizar la bitácora de atención de problemas para el departamento de HelpDesk.
- Revisar y determinar si el problema es en el Cache Flow, si lo es resolverlo lo más pronto posible.
- Si es el caso, llamar al proveedor de Internet (Andinanet), si el daño es en el ISP.
- Analizar el porque del problema ocurrido.
- Realizar el seguimiento de la solución al problema al departamento del HelpDesk.

Desastres de larga duración

Se denomina desastres de larga duración a aquellos problemas que por su efecto requieren poner en marcha el plan de supervivencia. Los posibles problemas que pueden convertirse en un desastre para la compañía se encuentran identificados previamente en el tema “problemas de corta duración”.

Las acciones de contención para dichos desastres son los siguientes:

Terremoto, incendio:

- De producirse un incendio o presencia de humo, se activarán automáticamente los detectores, los mismos que activarán las alarmas de cada piso, alertando sobre la emergencia. En el caso de un terremoto también se activaran las alarmas de cada piso.
- El Sistema de Seguridad instalado está configurado para desactivar automáticamente las puertas de cada piso, en caso de producirse una alarma.
- Sin embargo, las puertas de acceso a cada piso podrán ser activadas o desactivadas de forma manual a través de las llaves de seguridad existentes en cada piso.
- Los responsables de dicha actividad serán cada uno de los Líderes de Planta (1 por cada piso), los mismos serán los únicos responsables de poseer las llaves de seguridad.
- Estas llaves de seguridad son únicas para cada piso y solo pueden ser reemplazadas por la empresa que fabrica las puertas y sus seguridades.
- A su vez los Líderes de Planta guiaran al personal para evacuar por las escaleras durante el percance.
- Se disponen de suficientes extintores en cada piso como para sobrevivir al inicio de un flagelo incendiario, permitiendo alertar a los bomberos y controlar el fuego hasta su llegada.
- Los extintores de incendio podrán ser operados únicamente por el personal que ha sido capacitado durante los entrenamientos semestrales que brinda el Cuerpo de Bomberos a la compañía.
- Por cada piso existen al menos 2 personas que están en capacidad de operar los extintores mientras dure el percance.
- Se considera que por los efectos del desastre mencionado, no se dispone del Servidor Central ni del Servidor Backup, por tal motivo la compañía se encuentra sin comunicación, sin acceso a la información y sin acceso a los sistemas, es decir, se requiere poner en ejecución el plan alterno para Colombia mencionado en el Plan de Supervivencia. Además se debe continuar con lo estipulado en el tema “Problemas con los dos servidores”.

Problemas con los dos servidores:

- Al no disponer de los dos servidores por motivo del desastre entra en ejecución el plan de supervivencia inmediatamente después del plan de contención.
- Se ha establecido mediante un acuerdo mutuo entre Omnes de Colombia y de Ecuador que el servidor de datos de la ciudad de Bogotá dispondrá de un disco duro exclusivo de 45 GigaBytes de espacio, para almacenar información, proveniente de Ecuador en caso de producirse el desastre.
- Se procede a poner en marcha el plan de supervivencia por parte del comité de crisis conformado por:
    - Gerente General
    - Gerente de Sistemas y Comunicaciones.
    - Gerente de Seguridad.
- El Gerente de Sistemas procede a realizar la llamada a Bogota, para poner en alerta al personal de allá y preparar el Servidor.
- El Gerente General procede a comunicar a los empleados la vigencia del plan de supervivencia y el mecanismo alterno que permitirá continuar con las operaciones necesarias.
- El coordinador del departamento de HelpDesk, debe informar al personal el uso de las cuentas de VPN para el acceso a la red de SiNet, aclarando que las personas que no tengan una cuenta de VPN debe solicitarla con su respectivo Gerente de División.
- Los Gerentes de cada línea de producto serán los responsables de autorizar la creación de cuentas VPN para los usuarios que no dispongan del mismo.
- Se formará un grupo de trabajo conformado por 4 personas del departamento de HelpDesk, bajo la dirección del coordinador del departamento de HelpDesk. El grupo de trabajo mencionado será el encargado de configurar las cuentas de VPN acorde al “Manual de Instalación y Configuración de Redes Privadas Virtuales” en los equipos de los usuarios que dispongan de dicha cuenta.

- El administrador de la red será el encargado de preparar las cintas de respaldo que se restauraran en Colombia.
- El administrador de la red debe preparar la imagen correspondiente al sistema financiero para restaurar en Colombia.
- Se coordinará entre el Administrador de la red y el responsable del departamento financiero, la información con fecha posterior a la ultima fecha de respaldo de las cintas, que debe el responsable del departamento financiero ingresar manualmente en Colombia.

3.10.2. PLAN DE SUPERVIVENCIA

El coordinador “Fabiola Vejarano” del plan de Contingencias será la encargada de determinar si el daño existente es de características mayores para que en este caso se pase al plan de supervivencia como medida de mitigación ante el desastre, pasos a seguir.

Hardware

- Se recurrirán a los computadores de respaldo existentes en cada departamento.
- De producirse un daño en el servidor principal, entrará a trabajar el Servidor Backup, el cual, está haciendo réplicas constantemente del servidor principal.
- La puesta en operación del Servidor Backup se lo hace de manera lógica, reiniciando el mismo para que de esta manera entre a operar el Domain Backup, es decir para que suba el servicio DNS de respaldo.
- Las réplicas entre los dos servidores se las hace a través de un cable cruzado conectado a tarjetas de red secundarias en cada uno de los servidores. De esta manera, el tráfico entre los dos no influye en el tráfico normal de red del servidor principal y el secundario. De producirse un daño en todos los servidores, se pondrá en ejecución el la parte del Plan de Supervivencia correspondiente a Respaldos de la Información, que se encuentra detallado más adelante.

Software

- De producirse un daño en el sistema como tal, es decir en el código del mismo o su estructura, se deberá reinstalar el sistema con ayuda de los instaladores o sus programas fuente, los mismos que se encuentran en el armario del Cuarto de Servidores y una copia de cada uno en la Bóveda del banco junto los respaldos.
- Para la reinstalación de los sistemas se deberá sacar antes un respaldo de la información existente.
- En caso de detectar la presencia de virus informáticos en los computadores de cualquiera de los empleados y que el Software Antivirus halla fallado en la detección de los mismos, el empleado deberá notificar al departamento de HelpDesk y Soporte al Cliente.
- Ximena de la Vega obtendrá la actualización del antivirus Mcafee de la siguiente dirección http://www.mcafee.com/anti-virus/default.asp?, para posteriormente instarse en las estaciones de trabajo de la compañía.

Manejo de la Información

- La información almacenada en las cintas deberá extraerse hacia el servidor de dónde provenga la misma. Las cintas deberán ser extraídas de la bóveda del banco previa disposición administrativa por parte del Departamento de HelpDesk y Soporte al Cliente.
- Para el caso de una pérdida total de la información en los servidores, los respaldos más actualizados serán copiados inmediatamente en los discos duros de los servidores (en caso de requerirse nuevos discos se comprarán discos SCSI de 18.5 GigaBytes cada uno).
- En caso de que la pérdida sea parcial, se reemplazarán los archivos dañados o perdidos en forma manual, es decir, se buscarán los mismos en las cintas de acuerdo a un previo análisis de daños. Este análisis deberá ser efectuado tanto por un empleado del Departamento de HelpDesk y Soporte al Cliente, como por un empleado del departamento afectado por el problema.

- Se ha establecido mediante un acuerdo mutuo entre Schlumberger de Colombia y de Ecuador que el servidor de datos de la ciudad de Bogotá dispondrá de un disco duro exclusivo de 45 GigaBytes de espacio, para almacenar información, proveniente de Ecuador en caso de producirse un desastre. Dicha información será tomada de las cintas de respaldo, las cuales serán facilitadas por personal de Ecuador mediante un viaje a Colombia en el momento del percance. Como se indicó la principio de este punto, el acuerdo es mutuo entre las dos partes, por lo que Ecuador se compromete a disponer de un disco duro de igual capacidad en su servidor, para uso de Bogotá en caso de crisis.
- Cada empleado estará en posibilidad de disponer de una cuenta para uso de la VPN (Red Privada Virtual) de Schlumberger, la misma que será creada de acuerdo a la necesidad del mismo. El Gerente de cada Línea de Producto será el único autorizado a solicitar la creación de la misma.
- Una vez creada la cuenta VPN, el empleado estará en la disponibilidad de utilizar los servicios de uno de los proveedores de Internet local que poseen las configuraciones apropiadas para que la Red Privada Virtual funcione correctamente.

PROVEEDOR	DIRECCION	TELEFONOS	PAGINA Web
Andinanet	Jorge Drom s/n y Gaspar de Villarroel	292-4207 1-800 -100100	http://www.andinanet.net
Access Internet	Av. República de El Salvador N34-183 y Suiza Edificio Torreazul piso 7	225-0905 1-800-222377	http://www.accessinter.net
Interactive	Av. 12 de Octubre y Lincoln. Edificio Torre 1492, oficina 605	2986-440	http://www.interactive.net.ec
SatNET	Av. Eloy Alfaro N32-641 y Rusia	224-5910	http://www.satnet.net

PROVEEDOR	DIRECCION	TELEFONOS	PAGINA Web
		292 1450 1-800 -728638	

Tabla 3.2 Principales proveedores de Internet a nivel del Ecuador

- El uso de la VPN permitirá a los empleados conectarse al servidor de Bogotá mientras dure la crisis, y de esta manera recibir información a través de una cuenta de e-mail creada en el servidor de esta ciudad denominada*:* quito-sos@bogota.oilfield.slb.com a través de la cual se podrá enviar y recibir información de Ecuador. Cabe indicar que de ser necesario se podrán abrir más cuentas de e-mail según sea el caso.

- La configuración de las cuentas VPN deberá ser realizada por el personal de HelpDesk en Quito y acorde a las instrucciones del "Manual de Instalación y Configuración de Redes Privadas Virtuales" existente en el armario del Cuarto de Servidores. Existe una copia de este manual en las oficinas de Bogotá.
- Las cuentas de e-mail temporales deberán ser configuradas en los computadores de las personas que lo utilizarán, esto es, instalando el sistema Eudora (Programa de recepción y envío de e-mails) en cada uno estos. Esta tarea será realizada por el personal de HelpDesk que esté en Quito. Cabe indicar que de ser necesario esta configuración se la deberá realizar en los computadores de los domicilios de los usuarios que poseen cuentas VPN.
- Una vez realizada la evaluación de daños, se procede a poner en marcha el Plan de Supervivencia por parte del Comité de Crisis integrado por las siguientes autoridades:
    - Gerente General.
    - Gerente de Sistemas y Comunicaciones.
    - Gerente de Seguridad.
- Se procede a realizar una llamada telefónica a las oficinas de Bogotá para poner en alerta al personal y preparar el servidor para que este reciba la

información, es decir, se alertará a Colombia sobre el viaje del equipo de trabajo hacia este país mientras dure la crisis.

- El equipo de trabajo que se dirigirá a las oficinas en Colombia estará conformado por las siguientes personas:
    - Administrador de la Red.
    - Un empleado del Departamento de HelpDesk.
    - empleado del Departamento Financiero.
- El equipo viajará a Bogotá inmediatamente después que el Plan de Supervivencia se ponga oficialmente en marcha.
- El Administrador de la Red será quien lleve consigo las cintas de respaldo y toda la documentación correspondiente a información ingresada horas antes del desastre. Esta información deberá ser ingresada nuevamente en Colombia únicamente en el caso de ser requerida durante la crisis.
- Los empleados designados por el Departamento Financiero serán los responsables de realizar cualquier ingreso de información correspondiente a Finanzas.
- El empleado designado por el Departamento de HelpDesk será quien se encargue de la instalación temporal del sistema financiero en el disco duro instalado en Bogotá. Para esto se utilizará una imagen del sistema, la cual será configurada en una partición de 1 Gigabyte de los 45 Gigabytes que dispone el mismo.
- La información de cada una de las Líneas de Producto, será extraída de las cintas de respaldo y será ubicada en carpetas con la misma estructura que se tiene en el servidor de Quito, este procedimiento lo hace automáticamente el software preinstalado en el servidor y que opera la DLT (Dispositivo de lectura de las cintas). Como se indicó anteriormente, de ser necesario escoger la información a restituir de los respaldos, este procedimiento se lo hará de forma manual entre el personal del HelpDesk y el Departamento afectado.
- Una vez copiada toda la información en el servidor de Bogotá (este proceso no deberá tomar más de 1 día), se notificará al personal de Quito

para que únicamente los empleados que posean una cuenta VPN, hagan uso de esta información instalada y configurada en Bogotá.

- Para el uso de las cuentas VPN, los empleados en Quito deberán conectarse a un proveedor local de los descritos anteriormente. Una vez conectados estarán en capacidad de transmitir o recibir información del servidor de Bogotá, así como podrán utilizar el correo electrónico dispuesto para este caso.
- Este Plan se mantendrá mientras dure la crisis, sin embargo el mismo está dispuesto para funcionar con eficiencia en un lapso de una semana.
- El Administrador de la Red será la persona encargada de copiar toda la información a cintas de respaldo una vez terminado el período de trabajo en Bogotá.

3.10.3. PLAN DE RECUPERACIÓN

El presente capítulo es de suma importancia ya que en éste se define los procedimientos y planes de acción a tomar para poder recuperarse y retornar a la normalidad en el caso de ocurrida un desastre informático. El cumplimiento de los procedimientos para la recuperación de un desastre informático debe ser la responsabilidad de la máxima autoridad del departamento de HelpDesk y Soporte al Cliente considerando las recomendaciones del Plan de Prevención.

Definición de las Fases después del Desastre

Es responsabilidad del departamento de HelpDesk y Soporte al cliente el controlar la ejecución de las fases después de ocurrido un desastre. Las cuales deben ser ejecutadas de la siguiente manera:

- Priorizar las actividades del plan de recuperación.
- Ejecución de las actividades para la recuperación.
- Retroalimentación al Plan de Prevención y Contención.

Cabe indicar que después de realizar todas las fases anteriormente dichas, las mismas que permitirán volver a la normalidad, se debe actualizar la bitácora

correspondiente al desastre ocurrido, estipulando las actividades de recuperación que se ejecutaron, para de esta forma cerrar el caso de desastre ocurrido.

Priorización de Actividades del Plan de Recuperación

El plan de recuperación contempla un plan de acción en forma general, considerando la dimensión del problema, de tal forma que la evaluación de los daños y su comparación contra el plan de recuperación, nos dará la lista de actividades prioritarias y urgentes que se debe realizar en la institución.

Ejecución de las actividades para la Recuperación

Para le ejecución de las actividades para la recuperación, implica la utilización de recursos de dos tipos:

- La recuperación del desastre utilizando los recursos de la institución.
- La recuperación del desastre contando con los recursos externos como empresas contratadas para mantenimiento correctivo preventivo, debiendo ceñirse a lo estipulado en el contrato, para no perjudicar el normal desenvolvimiento de la institución.

Las actividades a ejecutarse se han clasificado de acuerdo a los desastres más comunes que pueden presentarse en la institución y descritos en el plan de prevención.

Problemas de corta duración

Infraestructura Física

Descripción de las actividades de recuperación para la infraestructura física.

FALLAS DE LA RED UPS (ALTERNATIVA 1):

Caso: Cuando no se tiene energía eléctrica en las tomas de UPS, en los momentos de falla de suministro de energía eléctrica.

- Contactar al proveedor de la red de UPS para que asuma o repare alguna falla que el equipo presente.
- Verificar el correcto funcionamiento de la red de UPS.

FALLAS EN LOS UPS (ALTERNATIVA 2):

Caso: Cuando no se tiene energía eléctrica en el UPS, en el momento que se desconecta el mismo de la toma eléctrica.

- Contactar al proveedor del UPS para que asuma o repare alguna falla que el equipo presente.
- Verificar el correcto funcionamiento del UPS.

Hardware

Descripción de las actividades de recuperación para el Hardware.

PROBLEMAS CON LOS DOS SERVIDORES:

Caso: En el caso de que el desastre afecte en su totalidad el funcionamiento del Servidor Central y el de Backup, se debe poner en marcha la activación del sitio alterno (Plan de Supervivencia). Las actividades para restablecer los sistemas a su estado de funcionamiento normal están descritas en la parte de Desastres de Larga Duración.

PROBLEMAS DE UNO DE LOS SERVIDORES:

Caso: Cuando el servidor deja de funcionar correctamente por problemas en los dispositivos o por falla de la fuente de alimentación

Falla del Servidor Backup:

- Determinar si el daño es en algún dispositivo del Servidor o en la fuente de alimentación.

- Referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a la empresa contratada para el mantenimiento preventivo correctivo para que repare la falla del Servidor Backup.
- Verificar el correcto funcionamiento de los dispositivos del Servidor Backup.
- Activar el equipo nuevamente para que trabaje como Servidor Backup.
- Verificar que el Servidor Central esté replicando al Servidor Backup.

Falla del Servidor Central:

- Determinar si el daño es en algún dispositivo del Servidor o en la fuente de alimentación.
- Referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a la empresa contratada para el mantenimiento preventivo correctivo para que repare la falla del Servidor Central.
- Verificar el correcto funcionamiento de los dispositivos del Servidor Central.
- Desactivar el Servidor Backup que está funcionando como principal, y activarlo nuevamente como servidor de respaldo.
- Activar el servidor central nuevamente para que trabaje como

Servidor Principal.

- Verificar que el Servidor Central esté replicando al Servidor Backup.

DAÑO EN LOS DISCOS DUROS DE LAS ESTACIONES:

Diagnóstico: Cuando no reconoce el disco duro, o no se puede acceder al mismo.

- Ubicar el disco que presenta problemas.
- Referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a la empresa proveedora para reemplazar el disco duro de la estación.
- Restaurar la imagen estándar correspondiente al modelo del computador.
- Instalar el software de aplicación especifico del usuario que no conste en la imagen.

- Verificar el correcto funcionamiento del disco duro de la estación.

ERROR EN LA MEMORIA RAM DE LAS ESTACIONES:

Caso: Cuando se detiene el computador desplegando con error de memoria al ejecutar alguna aplicación o al iniciar Windows.

- Referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a la empresa proveedora para reemplazar las memorias por otras de iguales o similares características.
- Verificar el correcto funcionamiento de la memoria de la estación.

PERDIDA O DAÑOS GRAVES DE LAS LAPTOPS:

Caso: Cuando el cambio de la laptop es irremediable.

- Certificar la aprobación para el cambio de la laptop.
- Referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a la empresa proveedora para reemplazar la laptop por una de similares características.
- Restaurar la imagen estándar correspondiente al modelo de la laptop.
- Instalar el software de aplicación especifico del usuario.
- Verificar el correcto funcionamiento de la máquina.

Software

Descripción de las actividades de recuperación para el Software.

PROBLEMAS DE ACCESO A LA BASE DE DATOS DEL SAFIWIN EN EL SERVIDOR CENTRAL:

Caso: Cuando no se puede acceder a la base de datos del SafiWin a pesar de que la misma se encuentra operativa en el Servidor Central y que la estación cliente del SafiWin se encuentra en red.

- Ejecutar un diagnóstico previo.
- Contactar al proveedor del sistema SafiWin para que asuma o repare el problema en la base de datos.
- Restaurar el último backup correspondiente a la información de la base de datos si es necesario.
- Verificar que exista acceso a la base de datos del SafiWin.

PROBLEMAS DE ACCESO A LA BASE DE DATOS DEL SAP BASIS:

Caso: Cuando no se puede acceder a la base de datos del SAP Basis a pesar de que existe comunicación con el Servidor en Houston y que la estación cliente del SAP Basis se encuentre en red.

- Se diagnostica el problema y se contacta al HelpDesk en Houston para que asuma o repare el problema en la base de datos.
- Verificar que exista acceso a la base de datos del SAP Basis. Servidores:

PROBLEMAS DE SISTEMA EN EL SERVIDOR CENTRAL:

Caso: Cuando el Servidor no arranca correctamente, no se levantan los servicios y los mensajes de error no son de los dispositivos del Servidor.

- Realizar una reinstalación del sistema en el Servidor Central, esto es sin reemplazar los archivos existentes.
- Desactivar el Servidor Backup de principal, y activarlo nuevamente como servidor secundario.
- Arrancar el Servidor Central, y activarlo nuevamente como el servidor principal.
- Verificar su correcto funcionamiento.

PERDIDA O DAÑO DE LA INFORMACIÓN DEL SERVIDOR DE DATOS:

- Determinar con el usuario la última fecha que trabajo con los archivos correctamente.

- Identificar el cartucho de acuerdo a la fecha.
- Recuperar y copiar los archivos.
- Verificar que los archivos recuperados estén correctos.

PROCESOS INHIBIDOS EN EL SERVIDOR DE COMUNICACIONES (WINDOWS NT):

Caso: Cuando por instancias no determinadas el Servidor deja de trabajar, perdiendo los servicios de la red.

- En este tipo de evento es necesario bajar el servicio del servidor de comunicaciones y subirlo nuevamente.
- Verificar que exista comunicación a través del sistema de monitoreo.

DAÑO EN LOS ARCHIVOS DE SISTEMA DE LAS ESTACIONES:

Caso: Cuando Windows no inicia correctamente.

- Si es posible ingresar a Windows en modo prueba de fallos, y salvar la información necesaria del usuario que no se encuentre en el servidor de datos.
- Restaurar la imagen estándar correspondiente al modelo del computador.
- Instalar el software de aplicación especifico del usuario.
- Verificar el correcto funcionamiento del sistema operativo y de las aplicaciones.

DAÑO EN LOS ARCHIVOS DE APLICACIONES DE LAS ESTACIONES:

Diagnóstico: Cuando la aplicación no se inicia correctamente.

- Desinstalar la aplicación con problemas.
- Instalar nuevamente la aplicación.
- Verificar que la aplicación trabaje correctamente.

CASO DE VIRUS:

Caso: En caso de detectar la presencia de virus informáticos en los computadores de cualquiera de los empleados y que el Software Antivirus halla fallado en la detección de los mismos.

- El empleado deberá notificar al departamento de HelpDesk y Soporte al Cliente.
- El HelpDesk verificará si se dispone de la última actualización del antivirus en la computadora del usuario.
- El HelpDesk procederá a desconectar de la red la computadora infectada, por seguridad del resto de computadores.
- Si se comprueba que la computadora posee su antivirus actualizado, se buscará en Internet información acerca del virus y su forma de eliminación. Existe una gran variedad de virus que pese a tenerse la última versión del antivirus, este lo detecta pero no lo elimina, por esta razón las empresas ponen a disposición páginas en Internet especializadas en la cura a estos problemas.
- Si el antivirus no se encuentra actualizado, se procederá a actualizar el mismo para posteriormente correrlo y verificar si este logra eliminar el virus; caso contrario se buscará en Internet la cura, tal como se explicó en el párrafo anterior.
- Por seguridad, la computadora infectada no deberá ingresar a la red hasta haberse confirmado al eliminación del virus.
- Una vez eliminado el virus, se realizará una evaluación de los daños y de ser necesario se recurrirá a los respaldos para recuperar la información perdida.

Caso: En caso de que uno de los servidores se vea afectado por la presencia de virus informáticos y que el Software Antivirus halla fallado en la detección y/o control del virus.

- Pese a que los servidores siempre deberán tener actualizados el antivirus, si se comprueba que el afectado no lo dispone, se procederá a actualizar el mismo para posteriormente correrlo y verificar si este logra eliminar el virus.

- De no eliminar el antivirus el problema, se buscará en Internet información acerca del virus y su eliminación.
- Una vez eliminado el virus se procederá a evaluar los daños, de ser necesario se recurrirá a los respaldos para restituir información perdida.

Respaldos

FALTA DE ESPACIO EN EL SERVIDOR DE DATOS:

- Preparar el disco duro de ampliación.
- Insertar correctamente el disco duro en uno de los slots disponibles del Servidor de Datos, sin necesidad de Apagar el Servidor. El Servidor detectará éste automáticamente (en caliente).
- Verificar el aumento de espacio en el Servidor de Datos.

Comunicaciones

Toda pérdida de comunicación se la detecta por medio de alarmas que emite automáticamente el sistema de monitoreo de enlaces.

PERDIDA DE COMUNICACIÓN CON EL SERVIDOR:

Caso: Cuando ningún usuario tiene comunicación con el Servidor.

- Referirse a la garantía del Servidor si se encuentra dentro del periodo del mismo, caso contrario, informar a la empresa contratada para mantenimiento, para reemplazar la tarjeta de red del Servidor por otra igual o de similar característica.
- Verificar el correcto funcionamiento de la tarjeta de red.
- Desactivar el Servidor Backup que se encontraba de principal, y activarlo nuevamente como servidor secundario.
- Arrancar el Servidor Central, y activarlo nuevamente como el servidor principal.

- Verificar su correcto funcionamiento, y revisar en el sistema de monitoreo que exista comunicación nuevamente.

Caso: Cuando un área no tiene comunicación con el Servidor.

- Referirse a la garantía del hub correspondiente al área con problemas si este se encuentra dentro del periodo del mismo, caso contrario, contactar a la empresa proveedora para reemplazar el hub por otra igual o de similar característica.
- Instalar el hub.
- Verificar el correcto funcionamiento del hub, y revisar en el sistema de monitoreo que exista comunicación nuevamente en el área.

Caso: Cuando una estación no tiene comunicación con el Servidor.

- Referirse a la garantía del equipo si este se encuentra dentro del periodo del mismo, caso contrario, informar a la empresa contratada para mantenimiento, para reemplazar la tarjeta de red por otra igual o de similar característica.
- Verificar el correcto funcionamiento de la tarjeta de red, y revisar que la estación tenga comunicación con el servidor.

FALLAS EN LA CENTRAL TELEFÓNICA:

- Referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a Alcatel para que resuelvan el problema lo antes posible.
- Verificar el correcto funcionamiento de la central telefónica.

DESACTIVACIÓN DE LA COMUNICACIÓN A TRAVÉS DE LA INTRANET MUNDIAL DE SCLUMBERGER:

Caso: Para que la institución esté dentro de la intranet mundial de Schlumberger (SiNET), debe existir un enlace entre Schlumberger de Ecuador con

Schlumberger en Houston, el cual se lo hace por medio del proveedor de comunicaciones Impsat.

- Contactar a la empresa proveedora Impsat para que resuelvan el problema.
- Verificar que exista salida a la intranet mundial de Schlumberger por medio del sistema de monitoreo.

DESACTIVACIÓN DE LA COMUNICACIÓN SOLO A INTERNET:

- Contactar a la empresa proveedora de Internet (Andinatel) para que resuelvan el problema.
- Verificar que exista salida a Internet por medio del sistema de monitoreo.

Desastres de larga duración

En el caso de que el desastre afecte en su totalidad las instalaciones, y se requiere poner en marcha la activación del sitio alterno (Plan de Supervivencia). Las actividades para restablecer los sistemas en el Servidor Central y en el Servidor Backup a su estado de funcionamiento normal son las siguientes:

ACTIVIDADES A EJECUTARSE EN PARALELO AL PLAN SE SUPERVIVENCIA:

- Se conformará un grupo con el personal del departamento de HelpDesk, para trabajar durante el periodo de supervivencia, el mismo que será liderada por el Jefe de sistemas.
- Adquirir si es el caso, dos Servidores del mismo modelo de Servidores Dell que eran los equipos anteriores. A su vez verificar que se disponga de:
    - 512 MB de memoria RAM.
    - 45 GB de espacio en el disco duro.
    - El mismo tipo de tarjeta de red para la comunicación.
- El mismo tipo de tarjeta de red para las replicas con el servidor Backup.

- Preparar dichos Servidores en cuanto a la instalación física, conexiones eléctricas, conexiones de comunicaciones, cableado entre los dos servidores, etc.
- Ubicar los CDs para restaurar la imagen tanto del servidor central como del servidor backup. Dichas imágenes se encuentran en el anaquel correspondiente al Administrador de la red.
- Restaurar las imágenes en los servidores correspondientes. Para restaurar la imagen simplemente se debe colocar el CD imagen en la unidad lectora y reiniciar el equipo. Arrancará el servidor automáticamente del CD y comenzará la restauración de la imagen.
- Las imágenes que se dispone para los servidores, están creadas para restaurar todo el sistema, servicios y aplicaciones necesarios para trabajar correctamente.
- Se debe tomar en cuenta que las imágenes se restaurarán con la información que disponía el servidor hasta la fecha que fue creada dichas imágenes, es decir:
- No se contará con las cuentas de ingreso a red que fueron creadas después de la fecha de generación de la imagen.
- No se contará con las cuentas de email que fueron creadas después de dicha fecha.
- Ni con el correspondiente espacio en el servidor de datos para los usuarios creados después de la mencionada fecha.
- Se debe preparar la información de los usuarios que se disponía hasta antes de ocurrir el desastre, esto es cuentas de acceso a red, cuentas de email. Esta información el departamento de HelpDesk lo está generando mensualmente.
- A su vez, después de restaurar las imágenes correspondientes, determinar cuales son las cuentas de acceso a red y las cuentas de email que se dispone en el servidor central.
- De acuerdo al listado de cuentas antes del desastre, se debe ir creando aquellas cuentas de acceso a red y cuentas de email que hacen falta en el

listado de cuentas que se dispone en el servidor por producto de la restauración de la imagen.

- Para la creación de la cuenta de acceso a red, el username es el primer nombre más el apellido paterno, separado por un espacio en blanco.
- Para la creación de la cuenta de email, el username es la primera letra del nombre más el apellido paterno, unido.
- Se debe blanquear los password de todos los usuarios tanto de las cuentas de acceso a red como de las cuentas de email.
- Se ingresará como estándar de las nuevas claves la inicial del primer nombre más el apellido paterno unido.
- Las cintas más recientes correspondientes a información de correo, deberán ser extraídas de la Bóveda del banco previa disposición administrativa por parte del Departamento de HelpDesk y Soporte al Sistema. Estas cintas no fueron llevadas a Colombia.
- Restaurar las cintas de correo en el servidor central.
- Instalar el Sistema Administrativo Financiero SafiWin.

ACTIVIDADES A EJECUTARSE DESPUÉS DEL PLAN DE SUPERVIVENCIA:

- Luego de terminado el período de supervivencia, el administrador de la red que viajó a Colombia, debe realizar un backup en cintas de toda la información que se tiene en el disco asignado.
- Se debe realizar en Colombia el backup de la información de los usuarios en un juego de cintas y el backup de las bases de datos del SafiWin en otro juego de cintas
- Ya en Quito, restaurar el juego de cintas correspondientes a la información de los usuarios. Al restaurar esta información se creará automáticamente la misma estructura de carpetas de usuarios.
- Restaurar el juego de cintas de la información de las bases de datos del SafiWin.

- Obtenida la información de los usuarios, dar permisos de acceso de lectura y escritura a los usuarios a sus respectivas carpetas en el Servidor de datos.

Retroalimentación al Plan de Prevención y Contención

Una fase importante del plan de recuperación es la retroalimentación, éste tiene como fin el de optimizar el plan de prevención y contención original de acuerdo a una evaluación de la crisis que afrontó la institución. Esto es mejorando las actividades que tuvieron algún tipo de dificultad durante la crisis y reforzando los elementos que funcionaron correctamente. La retroalimentación se la puede plantear en cualquiera de las etapas del Plan de Contingencias, con el principal fin de estar listos para actuar frente a desastres o acontecimientos futuros.

IV.- CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUCIONES

Una vez desarrollado todos los capítulos planteados en un inicio y en base a un análisis profundo obtenido por la metodología aplicada para el desarrollo de planes de contingencia se obtuvo resultados que conllevan a concluir lo siguiente:

- Considero que el momento que se pensó en el desarrollo del presente plan ha sido totalmente oportuno, pues se ha detectado que existen un gran número de medidas que necesitan ser implementadas de inmediato.
- La gran cantidad de información que se manipula en archivos de formato Word, Excel, PowerPoint, Adobe Acrobat, Visio, como también la base de datos en SQL Server; cuentan con un sistema de respaldos apropiado y un almacenamiento apropiado de dichos respaldos, éstos se almacenan en sitios externos a la compañía tomando las precauciones necesarias en pérdida de información.
- En las circunstancias actuales y debido a su importancia, se deben implementar ciertos mecanismos en manejo de la información.
- Durante el desarrollo del presente plan, se han encontrado ciertas limitaciones de orden técnico y dirigencial, las cuales atentaron contra el normal desempeño del presente Plan de Contingencias.
- Los usuarios no deben tener derechos de administrador sobre sus computadores, esto provoca que una gran cantidad de errores del sistema operen producto de instalaciones defectuosas y sin control.
- Existen algunos sitios de exposición, los cuales deberían manejarse con mayor cuidado. Este es el caso de cuarto de servidores, sala de reuniones, etc. Que no se apegan a las mismas políticas y procedimientos en seguridad de la información de la compañía.
- El hecho de que la única empresa desarrolladora de software sea la encargada de otorgar el mantenimiento necesario al sistema financiero es un riesgo bastante alto, especialmente por los tiempos de respuesta.

- Los dos servidores de marca Dell (NT y NT-B), se encuentran con sus cinco discos duros capacidad máxima de cada servidor llegando a su máxima capacidad de almacenamiento.

4.2 RECOMENDACIONES

Con el afán de contribuir al logro de una mejor gestión en seguridad de la información y ampliar al mismo tiempo las posibilidades de sobrevenir por posibles desastres que le podrían afectar a la empresa se realiza las siguientes recomendaciones:

- El plan de contingencia desarrollado debe ser actualizado al menos una vez al año o a su vez cuando haya modificaciones en la clasificación de información, se agreguen nuevos sistemas o aplicaciones al inventario de sistemas críticos.
- Debe existir la predisposición y apoyo de todas las autoridades de la compañía al presente Plan de Contingencias, ya que es un beneficio directo para la organización y todos sus integrantes.
- Las políticas planteadas en el capitulo III deberán ser cumplidos sin excepción alguna, que tienen como objetivo prevenir los desastres en seguridad de la información.
- Tanto Ecuador, Colombia y Perú, deberán complementarse mutuamente como sitios alternos de trabajo, esto en el caso de producirse desastres de manera local.
- Los tres países deberán contar con un Plan de Contingencias individual que determine las diferentes actividades a seguir durante una crisis. Para esto se procederá a realizar un Estudio de Complementación Mutua.
- Se recomienda que una persona de Omnes Ecuador informe de los cambios que realice el equipo de SL-IT a las políticas en seguridad de la información y las ponga en práctica, a través de la actualización del Plan de Contingencia.
- Se debe actualizar las políticas de Respaldos, de tal manera contar con un plan de respaldos cuando una crisis se presente en la empresa.

- El soporte al Cliente deberá ser centralizado en HelpDesk, además únicamente este departamento estará en posibilidad de administrar el sistema operativo de cada computador, valiéndose de las herramientas de administración que Microsoft Windows 2000 Professional dispone.
- La instalación y configuración del software deberá ser realizado únicamente por el personal del Departamento de HelpDesk, esto para evitar daños en la información producto de la manipulación irresponsable de los usuarios.
- Se deberá revisar el contrato de mantenimiento del software financiero con la empresa desarrolladora, de tal manera de que se llegue a un acuerdo con la misma sobre la administración del sistema por parte del Departamento de HelpDesk y Soporte al Cliente.

GLOSARIO

LDAP Lightweight Directory Access Protocol) Protocolo de acceso ligero a directorios, es un conjunto de protocolos para acceder a directorios de información. LDAP está basado en la norma X.500, pero es significativamente más simple X.500 es diferente, LDAP se apoya del protocolo TCP/IP que es necesario para cualquier tipo de acceso a Internet.

Cache Flor Nombre de la compañía que los fabrica, el CacheFlow es un dispositivo transparente que se apodera del servidor. El dispositivo CacheFlow es usado por Omnes para proporcionar cache de HTTP y se accede a Internet vía ISP local.

SL- IT Equipo de informática o sistemas de Schlumberger encargado de dictar o regular normas y estándares para todo Schlumberger a nivel internacional en donde la empresa tenga sus locaciones acatarán las normas o estándares que se encontrarán actualizadas en la red SINet.

Router Dispositiva de red que opera en la capa 1,2 y 3, del modelo OSI proporciona los servicios de conectividad de red en el ambiente LAN/WAN en la capa de red.

SINet Red de información de Schlumberger que son el resultado de las colecciones de redes de Schlumberger de zonas locales e intercontinentales que son sólo para el uso interno.

SSO Funcionario de seguridad del sitio de Schlumberger responsable para QHSE de un sitio local.

UTP Cable par trenzado no blindado.

STP Cable par trenzado blindado.

PKI Infraestructura de claves públicas. Es un sistema de encriptación y administración de claves públicas

VPN Red privada Virtual. Una tecnología que les permite a los usuarios conectarse a una red de Internet, manteniendo la seguridad de la red.

QHSE La función del QHSE es asumir el papel de administrador y coordinador la responsabilidad de manejar la seguridad de información y los procesos en las unidades comerciales de Schlumberger.

SSL Secure Socket Layer Es un protocolo diseñado para proveer: Privacidad, Integridad de los datos entre dos partes comunicantes.

Site Lugar o "sitio" donde está instalado, o puede ser instalado, cierto equipo de computo.

Stand Alone "individual". Equipo de cómputo que no está interconectado a otros.

Sistemas, Funciones y Recursos Críticos. Elementos vitales para la operación de la organizacióny posiblemente para su supervivencia.

Trap Door. Es un conjunto de instrucciones que permiten a un usuario traspasar las medidas estándares de seguridad de un sistema.

Vulnerabilidad Susceptibilidad de un sistema una amenaza de ataque específico o evento dañino.

Plan de Recuperación de Desastres. Los pasos previamente planeados a realizarse que hacen posible la recuperación de una instalación de cómputo del negocio, de las aplicaciones procesadas ahí o de ambas. También llamado plan de Contingencia.

Planeación de Contingencia. El procedimiento de desarrollar un plan de respaldo para restaurar las operaciones del centro de datos y el negocio en el caso de un desastre o interrupción. También llamado planeación de recuperación de desastres.

Política de Seguridad. El grupo de reglas y regulaciones que dicta cómo una organización protege, maneja y distribuye información sensible.

Prevención. Realización de actividades para evitar la ocurrencia de un fenómeno y, en caso de que suceda, disminuir su impacto. Con la prevención se trata de intervenir en el proceso de producción de las calamidades.

Privacía de la información. Se refiere al derecho de los individuos y las organizaciones para determinar por ellos mismos cuándo, cómo y hasta qué punto se puede difundir a otros la información acerca de ellos.

Procedimientos de respaldos (Backup). Métodos usados para recuperar programas y archivos de computadora después de un desastre o falla del sistema.

Procesamiento crítico. Aplicaciones que han sido identificadas por ser tan importantes para la operación de la compañía que poca o ninguna pérdida de disponibilidad es aceptable.

Protección. El objetivo de la protección o reducción de riesgos consta de las acciones de prevención y mitigación. La protección se realiza en las fases de preparación y al principio de la fase de respuesta a los desastres.

Recursos Cualquier cosa usada o consumida mientras se realiza una función. Las categorías de recursos en este contexto son: tiempo, información, objetos (contenedores de información), o procesadores (habilidad de utilizar la información).

Recuperación Consiste en la fase de retorno, cuando ya ha ocurrido la calamidad. Con el eventual mejoramiento de la situación, se trata de reconstruir y mejorar el sistema afectado, planteando el objetivo de la recuperación. La recuperación, junto con las actividades previas de rescate, constituye, el objetivo general de restablecimiento. La restauración de capacidades e instalaciones de cómputo.

Riesgo. La disponibilidad de que un agente amenazador podrá atacar exitosamente en contra de una vulnerabilidad específica de un sistema.

Seguridad de Datos. Proteger los datos contra modificación, destrucción o divulgación.

Seguridad de la información. La protección de activos de información contra divulgación no autorizada, modificación o destrucción, o la incapacidad para procesar información.

Hot Site Centro de cómputo ya equipado con hardware que se utilizará en la recuperación de desastres.

Impacto. El impacto constituye la más importante característica de la calamidad. Es el daño a la empresa como resultado del evento dañino.

Llave de encriptación Una "palabra" (cadena de caracteres) que al aplicarse a un mensaje en lenguaje natural junto con un método de encriptación (por ejemplo una matriz de encriptación) produce un mensaje encriptado (cifrado o codificado).

Mitigación Disminución de los efectos de los impactos de las calamidades. Con la mitigación se trata de cambiar el estado y funcionamiento del sistema afectable para disminuir las consecuencias del impacto desastroso.

Cold Site Centro de cómputo listo para recibir hardware para recuperación de desastres.

Criptosistema de Llave Pública. Una metodología de encriptación que depende de 2 llaves: una pública (disponible a cualquiera que quiera encriptar información) se usa para el proceso de encripción, y una privada (conocida sólo por el propietario) se usa para el proceso de desencripción.

BIBLIOGRAFIA

Titulo: Seguridad de la información en sistemas de cómputo.
Autor: Luis Angel Rodríguez.
Titulo: Guía de Lan Times de Seguridad e Integridad de Datos.
Autor: Farley, Masic.
Titulo: Firewalls y la Seguridad en Internet.
Autor: Siyan Karanjit
Titulo: Linux Máxima seguridad.
Autor: Pretice-Hall.
Titulo: Manual de Seguridad para PC'S y Redes Locales
Autor: Cobb, Stephen.

WEBBILIOGRAFIA DE INTERNET

http://ciberconta.unizar.es/LECCION/SEGURO/INICIO.HTML
http://www.iec.csic.es/criptonomicon/default2.html
http://www.econ.uba.ar/www/departamentos/sistemas/plan97/tecn_informac/seoane/seoane/tp/rivoira/seguridad.htm
http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html(sitio de seguridad de informacion)
http://www.sisonline.com/
http://polaris.lcc.uma.es/~amg/VREC/
http://ns.map.es/csi/silice/Seg.html
http://www.map.es/csi/fr340001.htm
http://www.reuna.cl/central_apunte/apuntes/soc_info5.html
http://www.linux-tech.org/
http://www.ictnet.es/ICTnet/cv/comunidad.jsp?area=tecInf&cv=sgsi
http://www.ictnet.es/ICTnet/cv/recursoscom.jsp?area=tecInf&cv=sgsi&seccio=2
http://www.ictnet.es/ICTnet/registre/form_nou.jsp
http://www.lcc.uma.es/~gisum/seguridad/seguridad-es.html
http://www.cerias.purdue.edu/hotlist/(Informacion en INgles en todos los aspectos)
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
http://www.dti.gov.uk/mbp/bpgt/m9ba91001/m9ba91001.pdf

WEBBIBLIOGRAFIA DE SINet

http://security.slb.com/resources/intro-checklist.html
http://www.hub.slb.com/index.cfm?id=id22507
http://www.pki.slb.com/
http://tradecompliance.slb.com/movement/encryption/index.asp
http://security.slb.com/training/sso/incidents.html
http://security.slb.com/training/passwords.html
http://www.new-york.sl.slb.com/policies/software_duplication.html