Universidad de Buenos Aires

Facultades de Ciencias Económicas

Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Tema:

Análisis sobre la re-estructuración del área de tecnología en una empresa periodística

Autor:

Ing. GUSTAVO MORALES

Tutor:

Ing. Hugo Pagola

Co-Tutor:

Dr. Ing. Facundo Caram

Fecha de Presentación:

Cohorte: 2013

RESUMEN

El presente trabajo final para la carrera de Especialización en Seguridad Informática trata de un caso de estudio real dentro de un periódico donde, a partir de una nueva gerencia de sistemas y por encargo de la directiva de la empresa, se busca una mejora y modernización de toda el área informática de la compañía.

Dada esta oportunidad, y aprovechando la falta de un estudio previo en el tema, se realizó un análisis de la situación hasta el momento y así proponer, a partir del mismo, las mejoras necesarias para lograr un importante avance en la calidad de los sistemas informáticos para que se modernicen de manera correcta y segura, alineados con los estándares de seguridad de la información adecuados para este tipo de organización.

Para llevar a cabo la mejora deseada, se realizó un estudio considerando los activos [1] informáticos de relevancia, es decir aquellos recursos que posee la organización para que el negocio funcione y se logren los objetivos deseados, por ejemplo servidores, sistemas de bases de datos, sistemas de almacenamiento, software, equipos de interconexión, etc.

Una vez identificados los activos y los procesos, se realizó un análisis de riesgo donde se buscaron las amenazas y las vulnerabilidades que puedan afectarlos y a partir de la información recabada se construyó una matriz de riesgo para cada uno estos procesos críticos. Las matrices de riesgo permiten visualizar para cada activo las amenazas y las vulnerabilidades a la que pueden estar sometidos en cuanto a la confidencialidad, la integridad y la disponibilidad (*ver 4.1*), como así también en la mismas matrices se indican la contramedidas que pueden llegar a evitar esas amenazas y vulnerabilidades. *(ver 6.1.7)*

[1] Según la Norma ISO/IEC 13335-1:2004 Activo es aquello que tiene valor para la organización.

Este estudio buscó determinar el riesgo y el impacto para la organización, en caso de concretarse alguna de las amenazas encontradas, a la vez que nos ayudó a planear las salvaguardas correctas para cada proceso, concluyendo en la creación de un informe con las recomendaciones y el plan de acción adecuado que nos asegure la información y la continuidad del negocio de forma cuantitativa.

INDICE

1. Introducción

La Empresa estudiada es una editorial periodística que se encuentra actualmente en un proceso de reestructuración tecnológica. Debido a que una nueva administración se ha hecho cargo y, ante la evidente desactualización por obsolescencia en los sistemas de producción y administrativos, se decidió encarar un proyecto de modernización de los sistemas y procesos directamente involucrados en la producción.

Hoy, los mercados exigen la modernización de procesos, para generar seguridad por medio de la implementación eficiente y eficaz de nuevas tecnologías, con la finalidad de mantener la continuidad del negocio.

En el presente trabajo, se propuso estudiar y evaluar mejoras de seguridad y operativas en las áreas tecnológicas vinculadas directamente con la producción. Para ello, se trabajó en identificar los procesos críticos involucrados mediante un relevamiento exhaustivo. Posteriormente se realizó un análisis de riesgo, haciendo el análisis de la confidencialidad, la integridad y la disponibilidad de la información, como así también se analizó la continuidad operativa de los sistemas involucrados.

Uno de los mayores desafíos de este trabajo (dada la falta de planes, de políticas, escasa conciencia en materia de seguridad y la ausencia de herramientas) fue lograr el apoyo *sine qua non* tanto financiero como político de la gerencia de la empresa, ya que sin esto no sería posible la implementación de las mejoras que aseguraran concretar los avances deseados para la organización. Para concretar este objetivo fue importante construir y presentar un planteo realista, de buena calidad y convincente.

Se generaron recomendaciones para lograr la implementación de las medidas (políticas, cambio de hardware, configuraciones, etc.) necesarias para evitar los riesgos en los procesos críticos, en pos de asegurar la disponibilidad, continuidad e integridad de los mismos.

El trabajo se limitó a los procesos críticos y no incluyó otras mejoras como, por ejemplo, seguridad en desktops, seguridad en dispositivos móviles, seguridad física de toda la planta. Los mismos serán analizados en etapas posteriores.

A partir de los resultados del análisis, se generó un informe gerencial que fue presentado a la dirección de la empresa, con el objetivo de conseguir el apoyo y el financiamiento necesarios para las mejoras propuestas.

2. Objetivos y Metodología de Trabajo

Se buscó

- Efectuar el relevamiento de la situación actual de la infraestructura física de la Red y de TI que dan soporte a los procesos.
- Detectar los procesos y la información crítica.
- Analizar la seguridad y el riesgo sobre la infraestructura actual.
- Realizar un análisis de riesgo de los procesos críticos.
- Diseñar un plan de seguridad y de continuidad de los procesos críticos acorde a las necesidades de cada uno de ellos.
- Realizar un informe completo del estudio.
- Hacer una presentación formal de las políticas y recomendaciones que resulten del caso.
- Documentar avances y problemas encontrados durante todo el proceso.

Para ello

- Se entrevistó a todos los sectores interesados -Administración, Gerencia de RRHH, Compras, Distribución, Redacción y Armado-.
- Se identificaron y clasificaron los activos informáticos, como así también procesos involucrados en los sectores mencionados.
- Se analizó el riesgo sobre la información, los procesos y aplicaciones críticas detectadas.
- Se crearon las matrices de riesgo para cada proceso, señalando las amenazas, las vulnerabilidades y las propuestas de contramedidas para evitar riesgos.
- En el desarrollo de este proyecto, se usó material bibliográfico con información relacionada a los diferentes aspectos a tratados (Normas ISO, COBIT, Firewalls, VPNs, Windows Server, VMware, y otros).

3. Situación Actual

La empresa cuenta con una red interna de aproximadamente 200 PCs, incluyendo los diferentes servidores y dispositivos de almacenamiento de datos (storage). La estructura y el tamaño de la red actual no fue planificada desde un comienzo, la misma fue creciendo con los años a medida que se fueron informatizando los diferentes sectores de la empresa. Los recursos informáticos existentes son utilizados en forma interna y externa, ya que la empresa tiene oficinas, empleados y clientes externos que acceden y utilizan recursos internos.

Una compañía que quiere ser competitiva debe adecuarse a las nuevas tecnologías. Estas tecnologías, entre ellas el diario en la web, los sistemas de los procesos productivos y administrativos y las aplicaciones que respaldan a las necesidades de los empleados del diario (video, audio, mail, redes sociales y otros) requieren mayores prestaciones a las actuales, recursos e interconectividad.

Al mismo tiempo, aumentó la posibilidad de ataques, intrusión y robo de información de datos de producción, bancarios, personales y otros. La continuidad de los sistemas y el acceso a la información se vuelven esenciales ya que son fundamentales en los procesos productivos. Por lo tanto, la empresa debe tener las herramientas y las políticas adecuadas que aseguren las prestaciones, la seguridad y la continuidad operativa del negocio. El equipamiento y los sistemas usados deben ser los apropiados para poder hacer frente a las necesidades presentes.

Dado que la empresa no cuenta con políticas en la materia ni con ningún estudio previo sobre cuáles son los procesos e informaciones críticas y tampoco cuenta con el conocimiento de sus necesidades reales en el tema, se realizó un estudio completo de todos los procesos involucrados.

4. Marco Teórico

4.1 Seguridad de la Información

La Norma ISO/IEC 27002 define a la información como: ***"un recurso que, como otros importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida."***[2]

Para la norma, la seguridad de la información es la preservación de la confidencialidad, la integridad y la disponibilidad de la misma.

La misma norma define como:

Confidencialidad a la propiedad que esa información esté disponible y no sea divulgada a persona, entidades o procesos no-autorizados.

Disponibilidad es la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Integridad es la propiedad de salvaguardar la exactitud e integridad de los activos.

Los **activos** son cualquier recurso que tenga valor para la organización.

4.2 Procesos Críticos

Los procesos críticos o sensibles son aquellos altamente necesarios para que la organización pueda funcionar en forma correcta y lograr sus objetivos. Estos procesos son considerados activos de la información por lo tanto, como indica la norma, deben ser resguardados.

Estos procesos o sistemas no pueden interrumpirse y son los que demandan mayor atención al momento de diseñar nuestras políticas, generalmente estos procesos requieren una mayor inversión.

4.3 Análisis de riesgo

Según la Norma ISO/IEC 27002 el riesgo es ***"la combinación de la probabilidad de ocurrencia de un evento y sus consecuencias".*** Mientras que el análisis de riesgo según la misma norma es el ***"uso sistemático de la información para identificar fuentes y estimar el riesgo"***. [2]

Todos los procesos están expuestos a alguna amenaza que, según la ISO 27002, ***"es una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización"***. Esta amenaza explota alguna vulnerabilidad del sistema o proceso. [2]

La norma ISO 27002 define a la vulnerabilidad como: ***"una debilidad de un activo o grupo de activos que puede ser explotada por una amenaza".***

4.4 Metodología para la evaluación de riesgo

El análisis de riesgo debe ser realizado mediante una metodología que nos ayude a sistematizar los procedimientos y técnicas del análisis.

Existe una amplia variedad de metodologías que se emplean para este proceso (Magerit, Nist, Octave, Mehari y otras).

En este trabajo se eligió la metodología CRAMM (***CCTA Risk Analysis and Management Method***) creada por CCTA (Centra Communication and Telecommunication Agency) del Gobierno del Reino Unido en el año 1987 y cuya versión actual es la 5.2. [10]

Esta metodología es totalmente compatible con la norma ISO/IEC 27001.

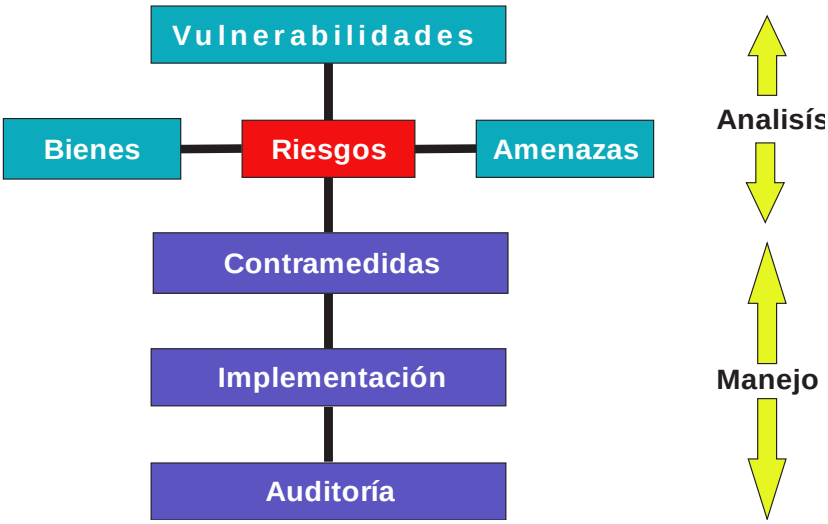


Figura 1: Etapas de la metodología CRAMM

(https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/)

La metodología CRAMM:

- *Provee un marco para calcular el riesgo desde el valor de los activos y sus vulnerabilidades, referido como Análisis de Riesgo (etapa de identificación y valoración de activos y la etapa de amenazas y evaluación de las vulnerabilidades)*
- *Dicho marco también ayuda a evitar, reducir o aceptar el riesgo, referido como Gestión del Riesgo (seleccionar y recomendar contramedidas o salvaguardas).*
- *Identifica y categoriza los activos en una de tres categorías:*

1) dato

2) aplicación /software

3) físicos.

- *Requiere considerar el impacto por la pérdida de confidencialidad, integridad y disponibilidad.* [9]

Fuente:[9] - http://www.itsmsolutions.com/newsletters/DITYvol2iss8.htm

5. Relevamiento de los procesos críticos

La empresa cuenta con diferentes sistemas informáticos para el desarrollo de su actividad.

Los principales procesos y sistemas analizados están vinculados a la producción, a las finanzas, a los recursos humanos, a las comunicaciones, al almacenamiento histórico de la información, a la seguridad informática y a la infraestructura de la red.

Tabla 1 - Listado de los sistemas, procesos analizados

ID	PROCESOS Y SISTEMAS
1	Sistema Editorial
2	WorkFlow (Paginado e Imposición)
3	Sistema de Ventas Avisos
4	Administración de Base Datos
5	LDAP Novell (Roles y permisos de Usuarios)
6	Infraestructura de red
7	Infraestructura de TI
8	Conectividad Remota
9	Administración de S.O. y Servidores
10	Sistema Gestión ERP
11	Sistema de RRHH
12	Sistema Help Desk (Mesa de Ayuda)
13	Servicios Contratados a Terceros
14	Sistemas de Antivirus
15	Sistema de Correo Electrónico

6. Análisis de Riesgo de los principales activos

En nuestro análisis, una vez identificados los procesos críticos, construimos diferentes matrices de riesgo para cada uno de ellos. Las matrices de riesgo son herramientas que permiten clasificar y visualizar los riesgos, mediante la definición de categorías de consecuencias y de su probabilidad (Norma ISO/IEC 31000). [4]

Cada proceso crítico fue identificado y analizado, recabando información de los usuarios y responsables de las diferentes áreas involucradas.

Para poder evaluar las posibles amenazas, vulnerabilidades y el impacto sobre la organización en caso de producirse algún incidente en cualquiera de los procesos estudiados, se reunió información por medio de una encuesta que se entregó a cada responsable de área y a los diferentes usuarios.

Luego, esa información recolectada y analizada se utilizó para crear las matrices de riesgo de cada uno de los procesos críticos anteriormente mencionados.

La técnica elegida para la construcción de estas matrices de riesgo se basó en la metodología CRAMM (ver 4.4).

6.1 Sistema Editorial

El sistema Editorial es un conjunto de aplicaciones y un sistema de bases de datos, que es usado por los redactores y cronistas de la Redacción para la crear el contenido periodístico del diario, tanto para su publicación en papel, como en internet.

Por lo tanto este sistema es la plataforma para crear su producto (el periódico).

Sin la información a la que se accede por intermedio del sistema, no hay materia prima para la creación del diario.

El soporte técnico a los usuarios y el mantenimiento del sistema es dado por el personal del área de técnica de la empresa y, con la firma que desarrolló el software (SoftData), se mantiene un convenio de asistencia y de actualizaciones.

Entre las diferentes aplicaciones que componen el sistema Editorial, las más importantes son:

6.1.1 SD-Editor

Este software es un editor de texto especialmente diseñado para periódicos. Para la edición en papel, el programa vincula los textos y las imágenes con las páginas (previamente se diagrama la forma y la posición dentro de la edición), permitiendo al periodista lograr la coincidencia del texto y ajustarse al espacio asignado dentro de la página, por lo tanto a medida que se escribe se puede saber si faltan o sobran caracteres. Para la versión digital en internet el software también puede vincular otros tipos de contenidos, como ser: videos, audios, hipertexto, etc.

Entre otras funcionalidades, podemos listar los siguientes elementos: corrector ortográfico, búsqueda en pantalla de cables noticiosos, y textos históricos, visualización del status las páginas o de la ediciones de cualquier producto, justificación y silabeo, edición simultánea, registro de históricos, asignación de trabajos y entrega de trabajos.

6.1.2 SD-ARC

Es un software mediante el cual se archiva todo el material deseado en formato digital (textos, fotos, infografías, videos, avisos, páginas y otros) que haya sido utilizado o no en la creación del periódico. Los contenidos almacenados son elementos de producción propia –generalmente notas y fotos- o los enviados por las agencias de noticias contratadas. Con el mismo programa se puede realizar la búsqueda de los materiales archivados y, luego de encontrado el elemento deseado, puede ser extraído de su lugar de almacenamiento para ser utilizado.

6.1.3 SD-Flow

Se trata de un software de diagramación de páginas (extensión para el programa Adobe InDesign, que se usa para la creación de páginas en formato digital). Con este programa se diagraman las diferentes ediciones para cada producto –diario y suplementos- que saldrá impreso en papel. Estos diagramas pueden ser reutilizados, por lo tanto los mismos son guardados en una base de datos específica, y desde donde luego pueden ser seleccionados para su reutilización (con o sin modificaciones).

6.1.4 SD-AdLayout

Esta aplicación se utiliza para el posicionamiento automático en páginas de publicidades y avisos comerciales (extensión de Adobe InDesign).

6.1.5 SD-WireService

Es un programa que realiza la recepción y la clasificación de los diferentes contenidos que envían las agencias de noticias, como por ejemplo notas, fotos e infografías.

6.1.6 Análisis de Riesgo

Por el tipo de producto que genera la empresa (todos los días sale a la venta un periódico diferente al del día anterior) y por la importancia que tiene este sistema en la elaboración del producto final, el Sistema Editorial es un proceso crítico, por lo tanto es fundamental su continuidad operativa, la integridad y confiabilidad, como así también la performance del mismo.

Es prioritario implementar acciones y controles tendientes a lograr los objetivos mencionados anteriormente para el sistema.

Activo : **Sistema Editorial**									
Propietario: **Área Periodística**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	4			8		10			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Virus**	**Errores de Entrada**	**Fallas de Discos**	**Falla de Alimentación**	**Falla de Enlace**	**Falla Sever SQL**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	4	5	5	8	9	7	2	8	7
Amenaza(1 a 100) Impacto X Vulnerabilidad	16	20	20	64	72	70	20	80	70
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Bajo	Bajo	Bajo	Medio	Alto	Alto	Bajo	Alto	Alto
Contramedidas	Mejora de Autenticación	Encripta-ción	Encripta-ción	Antivirus	Capacitación	Replicas y Backups	Redundancia/UPS	Redundan-cia de enlaces	Replicas y Backups

6.1.7 Explicación de la matriz de riesgo

La tabla anterior es la matriz de riesgo del Sistema Editorial, como se mencionó con anterioridad, la misma está basada en la metodología CRAMM, que es la metodología seleccionada para el trabajo.

En esta matriz se relacionan y valoran los diferentes aspectos que hacen a la seguridad de la información, ellos son: la confidencialidad, la integridad y la disponibilidad del sistema.

A cada uno de los aspectos se le da, dependiendo la importancia que tenga para el proceso, un valor de impacto; este valor va de 1 (ninguna importancia) a 10 (máxima importancia).

Para la confidencialidad existe un valor cero que equivale a que la información usada en el proceso es una información que puede ser pública, un valor de 1 a 5 cataloga a la información como restringida a aquellos usuarios del sistema que no tenga derechos completos sobre la misma. Por ejemplo, podrán visualizar, pero no podrán realizar hacer divulgación o modificación, un valor de 6 a 9 como confidencial y 10 indica que la información debe ser completamente segura.

El valor de la integridad se gradúa de la siguiente manera: si se considera relativamente bajo, varía de 1 a 3; cuando es moderado, varía de 4 a 7; si es alto, de 8 a 9; y, cuando consideramos que la integridad de la información debe ser muy alta, se valora en 10.

La necesidad de disponibilidad varía de 1 a 3, cuando se considera baja; de 4 a 6, moderada; de 7 a 8, alta; 9 cuando es muy alta; y 10 cuando es obligatoria.

Para cada aspecto mencionado anteriormente, se analizan qué amenazas pueden explorar las diferentes vulnerabilidades del sistema.

Estas vulnerabilidades se valoran de 1 a 10 dependiendo de la probabilidad de que esa vulnerabilidad sea explotada. Por ejemplo en este caso, la vulnerabilidad que tiene el sistema debido a la posibilidad de fallar la alimentación eléctrica se considera baja, ya que la empresa cuenta con sistemas redundantes, capaces de mantener la alimentación en forma ininterrumpida debido a la existencia de generadores eléctricos y

sistemas de alimentación ininterrumpida llamados UPS por sus siglas en inglés *"Uninterruptible Power Supply"*.

Mientras que el valor de un error de una entrada de datos es más alto, ya que dicha vulnerabilidad depende del factor humano.

El producto del impacto, por la vulnerabilidad, es el valor de la amenaza. Y el valor de la amenaza nos da el valor del riesgo. Se considera como un nivel de riesgo bajo cuando la amenaza varía de 1 a 33, medio cuando va de 34 a 67 y un valor alto de 68 a 100.

También para cada amenaza se plantea una alternativa de recomendación o contramedida. Por ejemplo, para evitar que la confidencialidad se vea afectada por la amenaza de la revelación, la contramedida propuesta es aumentar el requerimiento de los controles de autenticación, de forma que los usuarios o sistemas no autorizados no puedan acceder a los datos.

En definitiva, esta matriz nos provee la información de los aspectos que deben ser atendidos con mayor consideración y cuáles pueden ser las mejoras aplicadas.

6.2 WorkFlow (Paginado e Imposición)

Este sistema es el eslabón final de las etapas de pre-prensa (el siguiente paso es la impresión en la rotativa).

A partir del diagrama utilizado, el sistema realiza un chequeo continuo de las páginas de los diferentes productos (cuerpo principal, deportivo, suplementos, etc.) y a medida que las páginas se van completando genera una imagen de las mismas (ripeado), las rota y posiciona de la forma adecuada para la creación de las planchas offset que luego son necesarias para la impresión en la rotativa.

Las mencionadas planchas son creadas por equipos procesadores específicos para tal tarea, llamados CTP (de las siglas en inglés de la computadora a la plancha -*Computer To Plate*-).

Este sistema se compone de diferentes aplicaciones, la interface principal con el usuario es una aplicación web, por lo tanto además de un servidor de base de datos (SQL server) necesita un servidor Web.

6.2.1 Análisis de Riesgo

Para su funcionamiento el software requiere realizar un intercambio de información con otros procesos. De la base de datos del sistema editorial, obtiene la información sobre el estado de las diferentes páginas, y así comprobar si están completas o no. Con las aplicaciones que controlan cada CTP, consulta el estado de los mismos para saber si están ocupados –filmando- o libres, lo que habilita o no la copia de las planchas. También debe tener acceso al sistema de base de datos que usa la máquina impresora (rotativa), ya que el WorkFlow le pasa los porcentajes de las diferentes tintas (cian, magenta, amarillo y negro) por plancha y con esa información la rotativa hace un ajuste automático llamado pre-entintado que es un paso necesario para la correcta impresión de modo de reducir, en forma importante, la cantidad de diarios mal impresos.

Al igual que el sistema editorial, este es un proceso crítico: no es posible imprimir el periódico si el WorkFlow no funciona.

Activo : **WorkFlow**									
Propietario: **Área Taller de Diagramación y Fotomecánica**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	5			9		10			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Virus**	**Errores de Entrada**	**Fallas de Discos**	**Falla de Alimentación**	**Falla de Enlace**	**Falla Sever SQL**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	4	5	5	6	8	7	4	8	8
Amenaza(1 a 100) Impacto X Vulnerabilidad	20	25	25	54	72	70	40	80	80
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Bajo	Bajo	Bajo	Medio	Alto	Alto	Medio	Alto	Alto
Contramedidas	Mejora de Autenticación			Antivirus	Capacitación	Replicas y Backups	Redundancia/UPS	Redundancia de Enlaces	Replicas y Backups

6.3 Sistema de Ventas de Avisos

El sistema fue desarrollado por el área de Sistemas de la compañía y es utilizado para la toma, generación, armado y la facturación de los avisos clasificados.

Este posibilita vender diferentes tipos de avisos (lineales, destacados, con arte) en forma individual o secuencial. También aplica promociones o descuentos dependiendo de las ofertas, los paquetes vigentes o de los acuerdos especiales con los clientes.

Se vincula con el sistema editorial (SoftData), para la creación de pautas de publicación, para la verificación del espacio libre en las páginas que componen cada edición y para la colocación del aviso dentro dela página en forma automática, entre otras utilidades.

El soft cuenta con una interface con el sistema ERP para la facturación electrónica.

6.3.1 Análisis de Riesgo

Las agencias de venta se conectan en forma remota (por Internet) para ejecutar la aplicación y cargar los avisos. Por lo tanto, este sistema, además de depender de recursos como el servidor de base de datos y de un servidor de archivos, necesita una conexión estable y la velocidad adecuada de un proveedor de Internet ya que todas las receptorías de avisos externas se conectan simultáneamente por un período de tiempo prolongado.

Al ser un proceso en el que se realizan transacciones monetarias, se debe tener un adecuado nivel de seguridad, de forma que la información no pueda ser alterada o robada; a la vez que es necesario velar por la confidencialidad de los datos. Todos los eventos deben quedar registrados y su uso solo es posible para los usuarios debidamente registrados.

Activo : **Sistema de Ventas Avisos**									
Propietario: **Dpto. Comercial**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	5			10		10			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Errores de Entrada**	**Fallas de Discos**	**Falla de Alimentación**	**Falla de Enlace**	**Falla Sever SQL**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	4	5	5	5	7	7	2	8	2
Amenaza(1 a 100) Impacto X Vulnerabilidad	20	25	25	50	70	70	20	80	20
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Bajo	Bajo	Bajo	Medio	Alto	Alto	Bajo	Alto	Bajo
Contramedidas	Mejora de Autenticación			Firewall IDS	Capacitación	Replicas y Backups	Redundancia/UPS		Replicas y Backups

6.4 Administración de Base Datos

Los diferentes sistemas necesitan guardan datos que luego deben ser consultados y procesados en forma eficiente para lograr la funcionalidad de los sistemas involucrados. Estos datos se encuentran almacenados en varios servidores. Es por eso que existen varios gestores de bases de datos.

El sistema Editorial y el WorkFlow utilizan servidores SQL de Microsoft. El sistema de Avisos Clasificados, el Help Desk y otros usan el MySQL server de Oracle.

Mientras el sistema ERP y Facturación usan archivos de datos (DBase).

6.4.1 Análisis de Riesgo

La administración de base de datos incluye diferentes trabajos como ser el mantenimiento, réplicas, backups, restauraciones y otras tareas esenciales para el buen funcionamiento de los sistemas y la disponibilidad e integridad de los datos.

También se debe administrar y configurar la base de datos usuarios y los derechos de acceso.

Activo : **Administración de Bases de Datos**									
Propietario: **Sistemas**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	8			9		8			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Errores de Entrada**	**Fallas de Discos**	**Falla de Alimentación**	**Falla de Enlace**	**Falla Sever SQL**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	4	4	6	4	9	7	4	8	8
Amenaza(1 a 100) Impacto X Vulnerabilidad	32	32	48	36	81	56	32	64	64
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Bajo	Bajo	Medio	Medio	Alto	Medio	Bajo	Medio	Medio
Contramedidas	Mejora de Autenticación			Firewall IDS	Capacitación	Replicas y Backups	Redundancia/UPS	Redundancia de Enlaces	Replicas y Backups

6.5 LDAP Novell (Roles y permisos)

LDAP son las siglas en inglés de Protocolo Liviano de Acceso a Directorios. Éste protocolo permite a los usuarios y aplicaciones el acceso de los diferentes recursos disponible en la red.

En la actualidad, se usa un servidor con un sistema operativo de red llamado Novell Netware 6.5. Este servidor se sirve de una de base de datos propietaria llamada NDS (Novell Directory Services) o eDirectory, la misma se utiliza para representar los activos de la organización en un árbol lógico (unidades organizativas, usuarios, servidores, volúmenes, impresoras, etc.) y es donde se almacenan las políticas de accesos a los recursos (archivos, aplicaciones, datos y dispositivos), los roles y permisos para los diferentes grupos y usuarios.

6.5.1 Análisis de Riesgo

En el inicio de una sesión de trabajo, la conexión se establece mediante el uso de nombre de usuario y contraseña al servidor LDAP para poder realizar la tarea.

Al autenticarse al sistema, el usuario logra acceder a los distintos servicios ofrecidos (unidades de red, impresoras, correo electrónico, etc.) necesarios para realizar su labor diaria.

Las políticas de seguridad fijan qué utiliza cada usuario o grupo de usuarios y a qué recursos e información accede, por lo tanto estas políticas deben estar correctamente programadas.

Dada la importancia del sistema, es fundamental controlar la integridad referencial y mantener una réplica de la base y el sistema operativo en varios servidores.

Activo : **LDAP Novell (Roles y Permisos)**									
Propietario: **Sistemas**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	7			7		8			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Borrado**	**Fallas de Discos**	**Falla de Alimentación**	**Falla de Enlace**	**Falla en NDS**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	7	3	4	3	8	9	2	8	7
Amenaza(1 a 100) Impacto X Vulnerabilidad	70	30	40	30	80	90	20	80	70
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Alto	Bajo	Medio	Bajo	Alto	Alto	Bajo	Alto	Alto
Contramedidas	Mejora de Autenticación				Ajustar Permisos / Undelete	Replicas y Backups	Redundancia/UPS		Replicas y Backups

6.6 Infraestructura de RED

Llamamos infraestructura de red al equipamiento para la interconexión de equipos informáticos (*Switcher, Routers, Modems, Firewall, Access Point* para *WiFi*, etc.) y al cableado, ambos componen la llamada red de trabajo -*networking*-. Estos componentes son esenciales para el funcionamiento de toda la red, la cual se utiliza para el intercambio de datos y de las comunicaciones (externas e internas) de la empresa.

En el centro de datos (DataCenter) se encuentra el rack principal (mueble) donde se concentra el cableado de datos y los equipos que constituyen la infraestructura de *networking*.

6.6.1 Análisis de Riesgo

La disponibilidad y el buen funcionamiento de la infraestructura de red son esenciales para todos los procesos y sistemas existentes.

La configuración y el uso correcto del equipamiento son primordiales para mantener una infraestructura de *networking* segura.

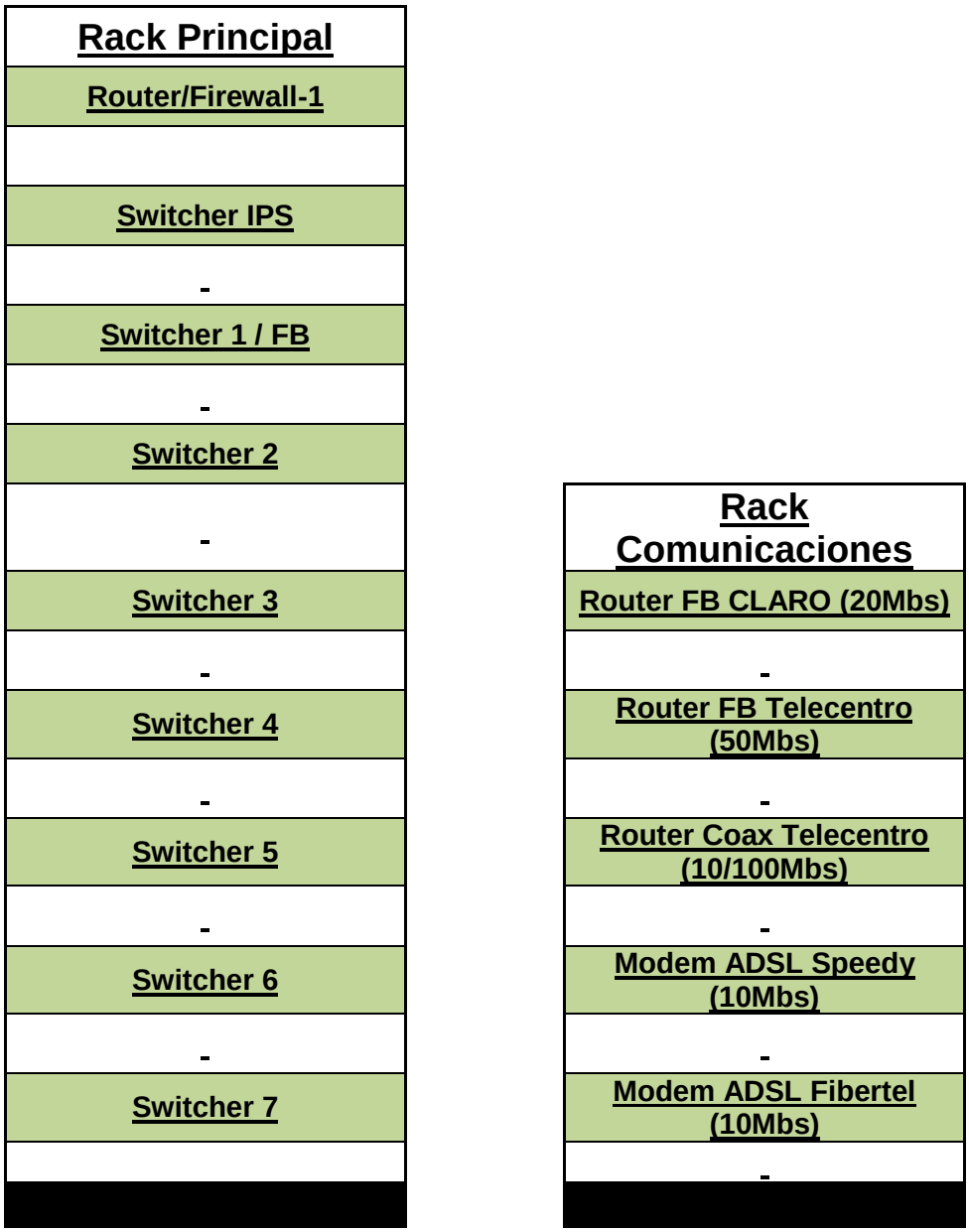
Los servidores que publican a la web, como ser los servidores de correo, de web o de FTP, deben estar en una zona especial llamada DMZ (siglas en ingles de zona desmilitarizada) de forma que los servidores y máquinas internas no puedan ser accedidas desde el exterior por alguien no autorizado (atacante).

De especial interés en la materia, es la seguridad de la red *WiFi*, donde una mala configuración –uso de claves débiles o protocolos de conexión antiguos- puede dar lugar a la existencia de una brecha de seguridad que puede ser aprovechada por un intruso para obtener acceso al sistema.

Por lo tanto para mantener la seguridad es necesario contar con diversos dispositivos de red -de hardware y de software- que permitan crear una defensa al sistema, como ser: *firewall* (corta fuego), servidores *proxy's* , IDS (sistema de detección de intrusos), IPS (sistema de prevención de intrusos) y otros dispositivo o herramientas necesarios para tal fin; todas ellos forman parte de esta infraestructura de red. Estos dispositivos además de existir en

la red deben usarse y configurarse en forma correcta para que cumplan su función.

Figura 2: Distribución de los Rack del DataCenter



Nota: El ***Switcher 1 / FB*** se interconecta por medio de un enlace fibra óptica de alta velocidad al **Rack 2** que se encuentra en el otro extremo de la planta -sala de CTP's- y al **Rack 3** en las oficinas de Administración.

Activo : **Infraestructura de Red**									
Propietario: **Sistemas**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	10			10		10			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Modificacio-nes**	**Fallas de Switchers**	**Falla de Alimentación**	**Falla de Cableado**	**Falla en Adaptado-res de red**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	3	3	3	3	8	8	2	4	7
Amenaza(1 a 100) Impacto X Vulnerabilidad	30	30	30	30	80	80	20	40	70
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Bajo	Bajo	Bajo	Bajo	Alto	Alto	Bajo	Medio	Alto
Contramedidas	Mejora de Autenticación				Controlar los derechos y privilegios de acceso.	Redundancia	Redundancia/UPS	Mantenimien-to y control	

6.7 Infraestructura de TI

La infraestructura de TI (tecnología de la información) la integran las aplicaciones y dispositivos (servidores, dispositivos de almacenamiento, computadoras de escritorio, impresoras, etc.) que alojan y brindan los servicios y la información necesaria a los distintos sistemas informáticos, procesos y usuarios.

6.7.1 Servidores

Esta infraestructura la constituyen veinticuatro de servidores con variedad de sistemas operativos (Windows, Linux y Novell).

El siguiente es un listado con las características y función de cada uno de los servidores actuales en la empresa:

Servidores				
ID	**Nombre**	**IP**	**S.O.**	**Servicios Principales**
1	Proxy_1	50.2	Windows 2003	Proxy/Mail Secundario/FTP/MySQL
2	Proxy_2	50.3	Windows 2003	Proxy/Mail Principal/FTP
3	Proxy_3	50.4	Windows 2003	Proxy/FTP/MySQL
4	IMPREBA-AC1	50.5	Windows 2008	Sistema de Avisos/Publicación WEB (IIS)/Terminal Server
5	Serv_IDRemoto	50.6	Windows 2008	Terminal Server (Ejecución remota del InDesign)
6	IMPREBA-SD1	50.7	Windows 2008	Sistema Editorial
7	IMPREBA-SQL1	50.8	Windows 2008	SQL Sistema Editorial
8	IMPREBA-SD2	50.9	Windows 2008	Sistema Editorial BackUp
9	IMPREBA-SQL2	50.10	Windows 2008	SQL Sistema Editorial BackUp
10	Serv-WebInterno	50.11	Windows 2008	Publicación WEB (IIS)/HELP DESK
11	Serv_Novell1	IPX	Novell 4.11	LDAP/File Server
12	Serv_Novell2	IPX	Novell 4.11	LDAP/File Server
13	Serv_Partes 1	50.12	Linux	Sistema de Partes de Producción/Publicación Web (Apache)/MySQL
14	Serv_Partes 2	50.13	Linux	Sistema de Partes de Producción/Publicación Web (Apache)/MySQL
15	ServAdm_1	51.2	Windows 2008	ERP Principal

16	ServAdm_2	51.3	Windows 2008	ERP Backup/File Server
17	ServQuilmes	50.14	Windows 2008	ERP AG. Quilmes
18	ServWeb	50.15	Windows 2008	Publicación WEB (IIS)
19	ServFileWeb	50.16	Windows 2008	File Server
20	ServWorkFlow1	50.17	Windows 2008	Sistema WorkFlow/SQL Server/IIS (Imposición)
21	ServRip1	50.18	Windows 2008	Servidor de Ripeo 1 (Conversión de PDF a TIFF)
22	ServRip2	50.19	Windows 2008	Servidor de Ripeo 2
23	ServRip3	50.20	Windows 2008	Sistema WorkFlow BackUp/SQL Server/IIS/Servidor de Ripeo 3
24	NAS_1	50.21	Windows 2012 Storage	NAS RAID (Archivo / Correos)

6.7.2 Dispositivos de Almacenamiento de Datos (Storage)

Los dispositivos de almacenamiento son componentes de hardware diseñados específicamente para almacenar un gran volumen de datos, generalmente en forma redundante (datos duplicados en diferentes lugares físicos) con gran velocidad de escritura y lectura. Son equipos externos a los servidores, por lo que varios servidores y usuarios pueden acceder a los datos almacenados en un mismo storage en forma simultánea.

Los modelos usados en la empresa son los denominados NAS (*Network Attache Storage*), estos dispositivos se conectan directamente a la red y poseen la capacidad de dictar políticas de control de acceso a los usuarios y a la información almacenada. Los NAS tienen una tecnología asociada llamada RAID (*Redundant Array of Independent Disks*), que en caso de producirse la falla de un disco que compone el sistema, la información no se pierde ya que los datos se encuentran escritos en forma redundante en otro disco. Existen distinta configuraciones posibles del sistema RAID, dependiendo cuál se elija varían las prestaciones y las seguridades del mismo, por ejemplo: una configuración que brinde mayor seguridad por lo general redunda en una menor performance y/o en una reducción en la capacidad de almacenamiento.

6.7.3 Análisis de Riesgo

Las vulnerabilidades que existen, tanto en los servidores como en los dispositivos de almacenamiento, pueden darse a nivel de hardware y de software asociado.

Entre los desperfectos de hardware más comunes podemos nombrar: fallas de discos rígidos (que además de ocasionar un caída de los sistemas, también puede acarrear pérdidas de datos, si estos no están duplicados en otro medio físico), fallas de alimentación (por corte de energía eléctrica o por desperfectos en las fuentes de alimentación), bloqueos por problemas de temperatura y perdida de conectividad (ver 6.6.1), entre otras.

Activo : **Infraestructura de TI**									
Propietario: **Gerencia de TI**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	5			7		10			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Virus**	**Fallas de Discos**	**Falla de Alimentación**	**Falla de Enlace**	**Fallos en S.O.**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	6	5	6	5	8	9	5	9	9
Amenaza(1 a 100) Impacto X Vulnerabilidad	30	25	30	35	56	90	50	90	90
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Bajo	Bajo	Bajo	Medio	Medio	Alto	Medio	Alto	Alto
Contramedidas	Mejora de Autenticación	Control de Acceso	Control de Acceso	Firewall IDS	Capacitación	Replicas y Backups	Redundancia/UPS	Redundancia de Enlaces	Manteni-miento

6.8 Conectividad Remota

Diferentes agencias externas, periodistas y usuarios administrativos se conectan en forma remota para hacer uso de aplicaciones, recursos y para la carga y descarga de diferente información. Por lo anterior, es esencial la seguridad y la disponibilidad de las comunicaciones.

6.8.1 Análisis de Riesgo

Para las interconexiones, la empresa cuenta con varios enlaces de Internet de diferentes proveedores. Esta variedad busca la redundancia de las conexiones para lograr la continuidad operativa.

La empresa cuenta con 2 enlaces dedicados (direcciones IP fijas) y simétricos (el mismo ancho de banda de subida y bajada) de 50 Mbits y un tercer enlace dedicado asimétrico de 100/10 Mbits que es utilizado para la navegación en Internet.

Y para asegurar dichas conexiones, se cuenta con diferentes elementos: el firewall de software (corta fuego que evita el trafico indeseable); y el proxy server (enrutador de paquete desde y hacia internet) que permite la navegación de los usuarios y aplica las políticas de seguridad para los mismos.

La empresa cuenta con un sistema de antivirus y antispam para los servidores de correo electrónico, además del antivirus corporativo para los puestos de trabajo.

Una falla en los dispositivos de seguridad, como así también una mala configuración de los mismos, puede ser utilizada por un hacker o un virus para acceder a la red interna de la empresa y así robar información o infectar los sistemas.

Activo : **Conectividad Remota**								
Propietario: **Área Periodística / Administración**								
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)		
Requisito de Impacto (1-10)	9			8		7		
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Errores de Comunica-ción**	**Fallas en el Enlace Físico**	**Falla de Alimentación**	**Ataque DDOS**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	8	8	7	9	7	7	2	9
Amenaza(1 a 100) Impacto X Vulnerabilidad	72	72	63	72	56	49	14	63
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Alto	Alto	Medio	Alto	Medio	Medio	Bajo	Medio
Contramedidas	VPN/ IPSec / SSL			Cifrado / Firma Digital		Replicas y Backups	Redundancia/UPS	

6.9 Administración de S.O. y Servidores

El hardware y los sistemas operativos (SO) usados para los servidores, tienen una elevada importancia en la infraestructura de la empresa, por lo que se debe tener especial cuidado en mantener la integridad, disponibilidad y performance de los mismos.

6.9.1 Análisis de Riesgo

Una mala configuración de seguridad o la falta de actualizaciones de los sistemas operativos o software utilizados pueden ser aprovechadas por un atacante (interno o externo) que puede robar o alterar información sensible, por lo tanto los sistemas operativos deben estar correctamente configurados y actualizados (antivirus, bloquear puertos y servicios no usados, políticas de control de acceso seguras –ACL-, etc.).

La falta de mantenimiento del hardware de los servidores podría ocasionar que estos se bloqueen inesperadamente por lo que los servicios prestados necesarios para la continuidad operativa dejarían de funcionar.

Activo : **Administración de S.O. y Servidores**									
Propietario: **Gerencia de TI**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	7			7		7			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Virus**	**Fallas de Hardware**	**Falla de Alimentación**	**Fallos de scripts**	**Fallos en S.O.**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	7	7	8	7	7	9	5	7	7
Amenaza(1 a 100) Impacto X Vulnerabilidad	49	49	56	49	49	63	35	49	49
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio
Contramedidas	Mejora de Autenticación	Control de Acceso	Control de Acceso	Firewall IDS	Capacitación	Replicas y Backups	Redundancia/UPS	Redundancia de Enlaces	Manteni-miento

6.10 Sistema ERP

El sistema de planificación de recursos empresariales ERP (Enterprise Resource Planning) provisto por la empresa Novamente, se utiliza para gestionar la producción, la facturación, la contabilidad, el stock y el inventario de la empresa.

Este cuenta con diferentes módulos para distintas funciones, entre ellos podemos nombrar los de ventas, facturación, cobranzas, compras y stock entre los más importantes.

6.10.1 Análisis de Riesgo

La información manejada por este sistema son datos sensibles, por lo tanto se debe garantizar su confiabilidad e integridad.

Según la norma ISO 27002:

"Se recomienda que los sistemas sensibles se encuentren en un ambiente informático dedicado (aislado)."

La recomendación anterior garantiza que solo podrán acceder los usuarios autorizados y desde el lugar que corresponda.

Activo : **Sistema ERP**									
Propietario: **Administración / Contaduría**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	10			10		7			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Errores de Entrada**	**Fallas de Discos**	**Falla de Alimentación**	**Falla de Enlace**	**Falla BD**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	10	8	9	10	8	7	2	8	7
Amenaza(1 a 100) Impacto X Vulnerabilidad	100	80	90	100	80	49	14	56	49
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Alto	Alto	Alto	Alto	Alto	Medio	Bajo	Medio	Medio
Contramedidas	Mejora de Autenticación			Firewall IDS	Capacitación	Replicas y Backups	Redundancia/UPS		Replicas y Backups

6.11 Sistema Recursos Humanos (RRHH)

El área de Recursos Humanos utiliza dos sistemas: uno para el control de acceso del personal, el cómputo de los días y las horas trabajadas y licencias del personal; y otro sistema para la gestión de colaboraciones periodísticas (pedido, aprobación, entrega y pago).

6.11.1 Análisis de Riesgo

La información manejada por este sistema se considera sensible, al igual que la manejada por el sistema ERP, por lo cual, las recomendaciones son las similares que las dadas anteriormente (ver 6.10.1), pero la información es menos sensible.

Activo : **Sistema de RRHH**									
Propietario: **RRHH**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	8			9		5			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Errores de Entrada**	**Fallas de Discos**	**Falla de Alimentación**	**Falla de Enlace**	**Falla BD**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	10	8	9	10	8	7	2	8	7
Amenaza(1 a 100) Impacto X Vulnerabilidad	80	64	72	90	72	35	10	40	35
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Alto	Medio	Alto	Alto	Alto	Medio	Bajo	Medio	Medio
Contramedidas	Mejora de Autenticación			Firewall IDS	Capacitación	Replicas y Backups	Redundancia/UPS		Replicas y Backups

6.12 Help Desk (Mesa de Ayuda)

La función de la mesa de ayuda es recibir pedidos de distintos tipos de servicio por parte de los usuarios de los diferentes sistemas. Estas solicitudes de servicio son dirigidas a diversas áreas dentro de la organización (Sistemas, Electricidad, Mecánica, Intendencia, Mantenimiento Primario y RRHH); los requerimientos se ingresan mediante una aplicación web desarrollada por el área de Sistemas.

Cada pedido se registra en una base datos y genera un ticket de servicio que es enviado al área o departamento que corresponda.

El progreso de la solicitud puede ser seguido, por el solicitante, en todas sus etapas hasta que se haya completado la misma.

6.12.1 Análisis de Riesgo

Este sistema permite obtener estadísticas de pedidos y fallas, por lo que es una herramienta útil para programar acciones de mantenimiento preventivo más eficaces.

Activo : **Help Desk (Mesa de Ayuda)**									
Propietario: **Gerencia de TI**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	6			7		8			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Errores de Entrada**	**Fallas de Hardware**	**Falla de Alimentación**	**Fallos en IIS**	**Fallos en SQL.**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	6	5	6	7	7	7	4	7	7
Amenaza(1 a 100) Impacto X Vulnerabilidad	36	30	36	49	49	56	32	56	56
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Medio	Bajo	Medio	Medio	Medio	Medio	Bajo	Medio	Medio
Contramedidas	Mejora de Autenticación	Control de Acceso	Control de Acceso	Firewall IDS	Capacitación	Replicas y Backups	Redundancia/UPS	Replica en otro servidor	Manteni-miento

6.13 Servicios Contratados a Terceros

Existen dos servicios de soporte contratados a empresas externas: uno, para el Sistema Editorial y el WorkFlow; y otro, para el Sistema ERP.

Las empresas externas (Softdata y Novamente) contratadas deben cumplir el alcance acordado en los contratos de servicios. En ambos casos el alcance incluye revisiones periódicas de funcionamiento y de backup, actualizaciones y/o modificaciones del software, asistencia técnica telefónica que con Softdata es 7x24 y con Novamente de lunes a viernes de 10 a 18hs. El sistema ERP incluye un acuerdo de confidencialidad para los datos.

6.13.1 Análisis de Riesgo

De ambos proveedores se pretende que cumplan la adecuada asistencia técnica que asegure la continuidad operativa en caso de contingencia y el respaldo de la información en ambos sistemas, entre otros temas (dentro de los alcances de nivel de servicios de cada contrato).

Esto debe ser monitoreado y controlado por personal de la empresa (Gerencia de TI).

Activo : **Servicios Contratados a Terceros**								
Propietario: **Gerencia de TI**								
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)		
Requisito de Impacto (1-10)	10			8		8		
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Errores de Entrada**	**Fallas de Asistencia**	**Fallo de Contingencia**	**Fallos de Resguardo**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	9	8	8	8	7	7	9	9
Amenaza(1 a 100) Impacto X Vulnerabilidad	90	80	80	64	56	56	72	72
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Alto	Alto	Alto	Medio	Medio	Medio	Alto	Alto
Contramedidas	Mejora de Autenticación	Control de Acceso	Control de Acceso	Firewall IDS	Capacitación	Replicas y Backups	Redundancia/UPS	Replica en otro servidor

6.14 Sistemas de Antivirus

Una de las mayores amenazas para cualquier compañía son los virus, malware y gusanos informáticos. Mantener la empresa libre de estas amenazas es de suma importancia para el buen funcionamiento de los sistemas.

La empresa cuenta con un sistema antivirus corporativo, este software debe instalarse en cada uno de los equipos conectados a la red de la empresa.

Mediante una consola de administración, se controlan, configuran y actualizan en forma remota el software antivirus de todas las estaciones.

También existe una solución de antivirus y antispam para revisar el tráfico de correo electrónico antes de que lo procese el servidor de correo.

6.14.1 Análisis de Riesgo

Las bases de datos deben ser sometidas a un control y mantenimiento periódico y, del mismo modo, las aplicaciones contratadas deben contar con los últimos parches o versiones; en ambos casos, para evitar posibles brechas de seguridad.

Activo : **Sistemas de Antivirus**									
Propietario: **Sistemas**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	5			9		9			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Borrado / Modificacio-nes**	**Fallas de Discos**	**Falla de Alimentación**	**Falla en Actualización**	**Falla BD**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	10	8	9	7	9	7	2	8	7
Amenaza(1 a 100) Impacto X Vulnerabilidad	50	40	45	63	81	63	18	72	63
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Medio	Medio	Medio	Medio	Alto	Medio	Bajo	Alto	Medio
Contramedidas	Mejora de Autenticación			Firewall IDS	Capacitación	Replicas y Backups	Redundancia/UPS		Replicas y Backups

6.15 Sistema de Correo Electrónico

La herramienta más usada para la comunicación interna y externa, así como también para el intercambio de datos, es el correo electrónico. Por esto, es de suma importancia la operatividad correcta y la disponibilidad del servicio de email.

Se cuenta con dos servidores de mail: uno principal y otro de contingencia.

6.15.1 Análisis de Riesgo

La integridad, la confidencialidad y la disponibilidad son ítems fundamentales para este sistema por lo que se debería tener un sistema antivirus y antispam adecuados. Del mismo modo, es necesario contar con enlaces de internet redundantes.

Activo : **Sistema de Correo Electrónico**									
Propietario: **Sistemas**									
	CONFIDENCIALIDAD pública (0), restringida (1-5), confidencial (6-9), segura (10)			**INTEGRIDAD** baja (1-3), moderada (4-7), alta (8-9, muy alta (10)		**DISPONIBILIDAD** bajo (1-3), moderada (4-6), alta (7-8), muy alta (9), obligatoria (10)			
Requisito de Impacto (1-10)	9			9		9			
Amenazas	**Revelación**	**Robo**	**Pérdida**	**Hackeo**	**Borrado / Modificacio-nes**	**Fallas de Discos**	**Falla de Alimentación**	**Falla de Enlace**	**Falla BD**
Vulnerabilidad(1-10) Ninguna (0), baja (1-4), moderada (5-7), alta (8-9), muy alta (10)	10	8	9	10	9	7	2	8	7
Amenaza(1 a 100) Impacto X Vulnerabilidad	90	72	81	90	81	63	18	72	63
Nivel de riesgo Bajo (1-33), Medio (34-67), Alto (68-100)	Alto	Alto	Alto	Alto	Alto	Medio	Bajo	Alto	Medio
Contramedidas	Mejora de Autenticación			Firewall IDS	Capacitación	Replicas y Backups	Redundancia/UPS		Replicas y Backups

7. Recomendaciones

Las siguientes conforman una serie de recomendaciones que surgen del relevamiento de los procesos críticos y del análisis de riesgo.

7.1 Planes de continuidad del negocio

Se propone la implementación de un plan de continuidad del negocio (BCP siglas en inglés) que defina las políticas, acciones e instrumentos necesarios para asegurar el funcionamiento continuo de los procesos y sistemas, como la disponibilidad de la información que conforman la actividad principal de la compañía (núcleo del negocio).

Se trata de poder definir una estrategia llamada DRP (de las siglas en inglés plan de recuperación ante un desastre) que determine la capacidad de una organización para continuar con sus operaciones a un nivel aceptable luego de un incidente (ISO/IEC 22301). Específicamente, en el caso del diario, los tiempos de recuperación aceptables varían según el sistema afectado y el horario en que se produzca el incidente. Por ejemplo, una caída del sistema editorial próximo al horario del cierre de la edición –a las 23 hs.- es mucho más crítica que una caída a las 17 hs. A la hora de cierre, el sistema debería volver a funcionar a lo sumo unos pocos minutos (10 o 15) después de producirse la falla.

Dado lo expuesto, se deben adoptar medidas que mitiguen los riesgos además de planear las acciones necesarias para la recuperación dentro de los tiempos donde el impacto negativo sea aceptable para la organización.

Ya que se identificaron los procesos críticos y sus riesgos, conocemos cuáles serán tomados en cuenta para nuestro plan. No trataremos de eliminar los riesgos ya que implicarían soluciones muy costosas (por arriba de u$s 40.000.-), sino que trataremos de aceptar estos riesgos y limitarlos tomando las medidas adecuadas (backups, réplicas, clusterización de servidores, firewalls, UPS, etc.).

7.2 Disponibilidad y tolerancia fallas

Es de suma importancia que el Sistema Editorial se encuentre disponible en todo momento y, como se mencionó anteriormente, en particular en los horarios de cierre de edición. De este modo y para cumplir el objetivo, se sugiere la implementación de las medidas que permitan lograr un sistema con alta disponibilidad. Por ejemplo, la demora que pueda llegar a producirse en caso de existir una falla en el sistema puede dar lugar a una situación crítica ya que hay una fuerte dependencia entre el comienzo de la impresión y la buena distribución y cantidad de ejemplares vendidos. Por ejemplo, los diarios que se distribuyen para su venta en el interior del país (10% de la producción) se envían vía área, esos vuelos son en un horario fijo (1:30 hs.) y, en caso de que se demore el arranque de la impresión por los motivos que fueran –entre ellos una falla en el sistema editorial- esos diarios no se distribuirían, por lo tanto no se venderían. Algo similar pasa con la distribución en las zonas más alejadas del conurbano, esto se debe a que la empresa externa que se encarga de la distribución no envía los camiones pasadas las 3:30 hs.

Actualmente el sistema se implementa en dos servidores: uno donde se alojan las aplicaciones y los archivos, y otro servidor que opera el servicio de bases de datos. A su vez, cada servidor cuenta con una máquina física gemela de backup, donde se están replicando los archivos y los datos, en forma continua.

Lo anterior brinda un respaldo ante la caída o falla de alguno de los servidores principales, sin embargo existen ciertos inconvenientes operativos. Entre ellos, el de la necesidad de monitorear, en forma periódica, el correcto funcionamiento de las réplicas. Por otro lado, el cambio de un servidor a otro no es sencillo (se debe cambiar la configuración de dirección IP y nombre) y no es automático por lo que se suma un problema: la reconfiguración de los servidores debe ser realizado por personal técnico especializado y el tiempo que se demora en la puesta en marcha es considerable; en particular, en el horario pico de la producción (horario de cierre de páginas) el problema se ve aumentado.

El problema anterior se soluciona (luego de estudiar el tema y las diferentes tecnologías existentes en el mercado) implementando la virtualización de servidores, además del agregado de herramientas de software, de forma de lograr una alta disponibilidad tanto para los servicios, aplicaciones, archivos y bases de datos.

La mejor opción se encontró en la solución dada por la firma ***VMware***, con su aplicación ***VMware vSphere*** y los módulos ***High Availability*** y ***Fault Tolerance*** (para alta disponibilidad y tolerancia a fallas) con la combinación del hardware adecuado (servidores y dispositivos de almacenamiento).

"VMware vSphere® brinda máxima disponibilidad para su entorno virtualizado, lo que hace que el tiempo fuera de servicio planificado sea una preocupación del pasado. Además, minimiza el tiempo fuera de servicio no planificado mediante el reinicio automatizado de las máquinas virtuales. Gracias a la automatización de la ubicación de las máquinas virtuales y el equilibrio de carga, el respaldo y la recuperación, junto con la recuperación ante desastres de todo el sitio, aumenta aún más la disponibilidad"[2].

7.2.1 Alta Disponibilidad (High Availability)

"vSphere High Availability (HA) brinda la disponibilidad que necesita la mayoría de las aplicaciones que se ejecutan en máquinas virtuales, independientemente del sistema operativo y de la aplicación que se ejecute. HA brinda una protección de conmutación de recuperación uniforme y rentable contra interrupciones en el hardware y el sistema operativo dentro de su entorno de TI virtualizado. HA puede realizar lo siguiente:

Monitorear las máquinas virtuales y los anfitriones[3] vSphere para detectar fallas del hardware y de los sistemas operativos invitados

Reiniciar máquinas virtuales en otros anfitriones de vSphere en el clúster[4] sin intervención manual cuando se detecta una interrupción en un servidor

[2] ***http://www.vmware.com/ar/products/vsphere/features/availability***

[3] ***Los anfitriones son las máquinas físicas donde residen las máquinas virtuales.***

[4] ***El clúster es el grupo de máquinas físicas.***

Reducir el tiempo fuera de servicio de las aplicaciones, ya que reinicia automáticamente las máquinas virtuales cuando se detecta una falla en el sistema operativo"[5]*.*

7.2.2 Tolerancia a fallas (Fault Tolerance)

"VMware vSphere Fault Tolerance (FT) brinda disponibilidad continua para las aplicaciones y protección contra fallas en el hardware mediante la creación de una instancia activa secundaria de una máquina virtual que se encuentra en sincronía virtual con la instancia principal. Gracias a la conmutación de recuperación inmediata entre esas dos instancias, FT elimina incluso la mínima posibilidad de una interrupción o pérdida de datos"[6]*.*

Lo anterior es posible ya que existe una réplica exacta de la máquina virtual en otro host físico y el sistema monitorea en forma constante sí la máquina virtual no está caída.

Este software no solo es una solución para el Sistema Editorial, sino que también puede considerarse como una solución integral para la organización ya que, si se adquiere el hardware adecuado, se podrá virtualizar la mayoría de los servidores en uso y, de esta forma, lograr que todos o la mayoría de los sistemas tengan alta disponibilidad y tolerancia a fallas.

7.3 Políticas de resguardo (backup) y recupero de información

Definir e implementar las políticas de resguardo ayudan a evitar pérdidas de información de forma que, llegado el caso, sea posible su recuperación y a su vez mantener la autenticidad de los datos. Como ya se mencionó, estos datos son activos para la organización.

Las correctas políticas de recuperación sirven para proteger los datos resguardados, es decir, la confidencialidad, integridad de los mismos.

La norma ISO/IEC 27002 recomienda hacer una clasificación de los activos, por lo que es necesaria una clasificación de la información. De este

[5] ***http://www.vmware.com/ar/products/vsphere/features/high-availability.html***

[6] ***http://www.vmware.com/ar/products/vsphere/features/availability#sthash.s8RrDZoo.dpuf***

modo, se asegura que la información reciba el grado de protección de acuerdo a la sensibilidad y criticidad de la misma, de forma de definir los tratamientos a utilizar en cada caso para conseguir el objetivo. La clasificación debe ser por área o proceso, por tipo de información (administrativa, confidencial, no confidencial, de producción -páginas, fotos, notas-, contratos, manuales, software, licencias, tipo de archivo, mails, etc.) y por el tipo de archivo (base de datos o archivo).

7.4 Tareas de Respaldos de la Información (BackUp)

Se propone implementar diferentes tareas de respaldo de la información en forma automática (base de datos, mails, información contable y periodística) y poner especial énfasis en las que incumben a los procesos más críticos, a la vez de reorganizar las ya existentes.

Actualmente, se hacen a diario copias programadas de las casillas de correo electrónico, la réplica de las bases de datos del Sistema Editorial y del Sistema de Avisos Clasificado. También se hacen backup de los archivos de uso (páginas, textos e imágenes) del sistema editorial.

Se detectó que no hay programado un backup de las bases ni de los archivos del Sistema ERP. Esta responsabilidad fue delegada a la empresa contratada para administrar el sistema; cuya administración se hace en forma remota, pero no hay un control sobre su correcta implementación.

Tampoco son supervisados, en forma continua, los diferentes backups que hacen los empleados de diferentes áreas, entre las que podemos nombrar RRHH, Compras y Contaduría.

No hay un plan de recuperación ni de resguardo de la información respaldada. Por lo tanto es necesario realizar un plan por el cual se defina quién o quiénes son los responsables de dichas tareas.

Se propone, entonces, implementar la automatización de los backups no existentes en la actualidad y que los responsables asignados sean los encargados de verificar la validez de los datos resguardados, de forma de garantizar que los datos relacionados a todas las bases (Editorial, WorkFlow, ERP, RRHH y Clasificados) y archivos de datos esenciales para la continuidad operativa tengan un respaldo adecuado.

7.5 Políticas de control de acceso y seguridad de la información

Las políticas de control de acceso pretenden asegurar que los servicios y datos de la organización sean usados y consultados por los usuarios indicados, la norma ISO/IEC 27002 aclara que el objetivo es: "***Asegurar el acceso a los usuarios autorizados y prevenir el acceso no autorizado a los sistemas de Información"[7].***

La seguridad en la información trata de proteger la integridad, la disponibilidad y la confidencialidad de los datos.

El control de acceso es tanto lógico como físico (ISO/IEC 27002). El acceso lógico es el que se produce cuando los usuarios acceden al sistema, generalmente con nombre de usuario y contraseña.

El control del acceso físico trata de proteger aquellos lugares de importancia como, por ejemplo, el Datacenter de las personas, donde intencional o accidentalmente se pueda llegar a producir un incidente que provoque un fallo, poniendo en riesgo la operatoria de la organización.

"Las personas son esenciales para operar un centro de datos; sin embargo, investigaciones realizadas coinciden en que las personas son directamente responsables del 60% del tiempo de inactividad de los centros de datos. Las personas provocan accidentes y cometen errores, entre los que pueden nombrarse aplicación de procedimientos inadecuados, rotulación incorrecta de equipos, caída de elementos y derrame de líquidos, errores en el ingreso de comandos, y otros contratiempos de mayor o menor trascendencia. Dado que el error humano es una consecuencia inevitable de la presencia de personas, minimizar y controlar el acceso del personal a las instalaciones es un elemento esencial en la gestión de riesgos, incluso cuando el riesgo de actividades maliciosas es mínimo"[8].

7 Norma ISO/IEC 27002 – Sistemas de Gestión de la Seguridad de la Información – Código Buenas Prácticas

8 APC (American Power Conversion) – Informe Técnico N° 82 – Seguridad Física en Instalaciones de Misión Crítica - Revisión 2. (por Suzzane Niles)

El primer paso es identificar qué se debe proteger, es decir, cuáles son los sistemas y las áreas físicas que requieren algún tipo de seguridad para acceder a ellos.

El siguiente paso es definir el criterio de acceso, es decir, quién debe acceder, el motivo del acceso y qué debe llegar a conocer.

Existen tres métodos de identificación de las personas:

- Lo que la persona tiene.
- Lo que la persona conoce.
- La identidad de la persona.

Lo que la persona tiene es de baja seguridad (llave, tarjeta, etc.) ya que puede ser robada o pasada a otra persona.

Lo que la persona conoce es de mayor seguridad que el anterior pero no es muy seguro, ya que la información puede llegar a compartirse o dejarse por escrito (contraseñas, códigos de procedimientos, etc.).

La identidad de la persona es de máxima confiabilidad, pero requiere de equipamiento más costoso y a veces puede llegar a ser intrusivo (huellas digitales, reconocimiento de iris, retina, facial, voz, etc.).

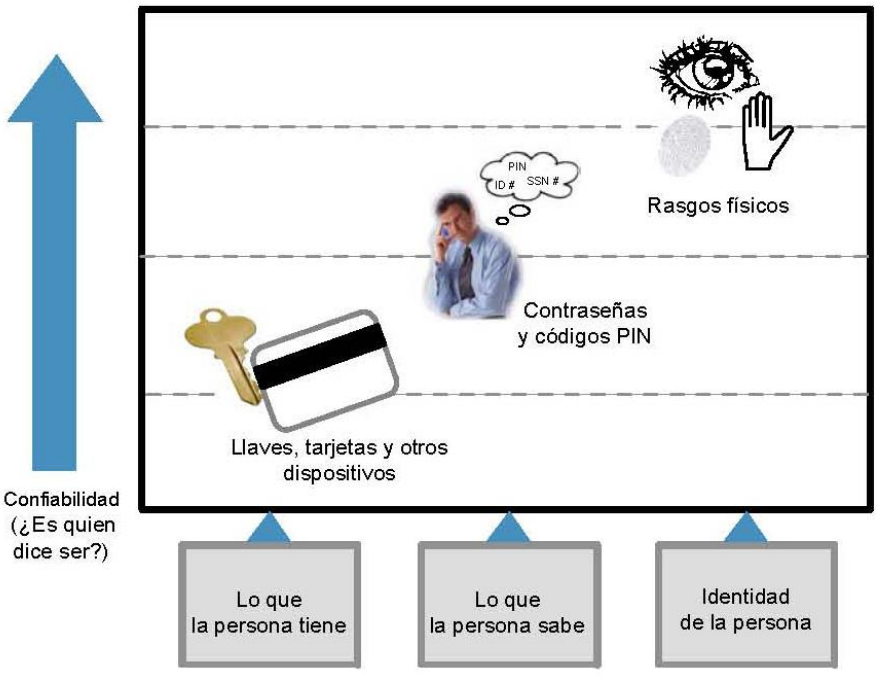


Figura 3: Métodos de Identificación (Fuente APC – Informe Técnico N° 82) [8]

La empresa no cuenta con políticas claras de control de acceso, por ejemplo las contraseñas de usuarios no vencen, no se verifica la robustez de las mismas (claves cortas o con caracteres repetidos o en secuencia simple son comunes) y las mismas, muchas veces, son compartidas.

Cierta información sensible (financiera y de recursos humanos) no está debidamente resguarda ya que es almacenada en carpetas de acceso público, no se controla de manera adecuada quién puede o no acceder a esa información.

Tampoco se tiene implementado un control de acceso al Datacenter, ya que el mismo no tiene cerradura con código y tampoco queda registro de ingreso de personal alguno.

Debido a los puntos anteriores se recomienda implementar políticas que obliguen a los usuarios al cambio periódico de contraseñas, solicitar la confidencialidad de las mismas y rever los controles de accesos lógicos -endureciendo las políticas de control actuales-, y físicos –por medio de sistemas biométricos- a aquellos sistemas y lugares que manejan información sensible.

7.6 Estrategia de seguridad en la red

La red de datos actualmente es protegida por la implementación de un firewall de software (aplicación que bloquea el tráfico no deseado) y de proxys servers para la navegación, donde se definen las políticas del uso de Internet.

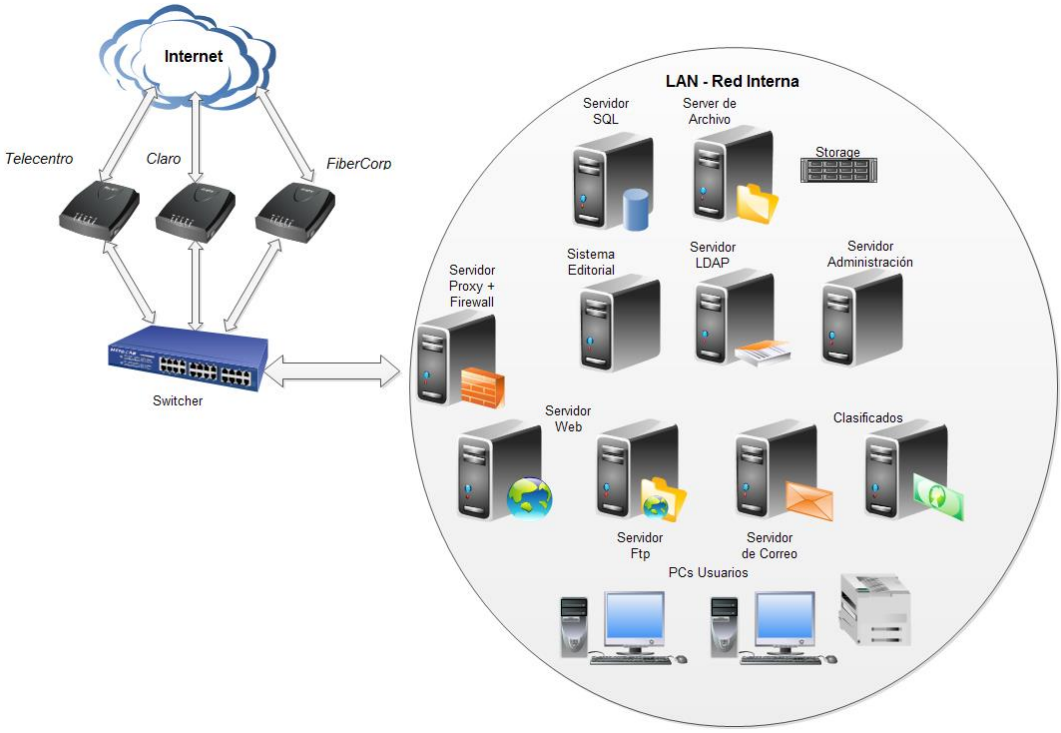


Figura 4: Esquema topológico de la red actual

Para agregar seguridad a la red interna (LAN) se recomienda la implementación de las siguientes medidas:

7.6.1 Defensa por capas

Para una mayor seguridad se puede separar la red interna, creando diferentes segmentos (subnet) por medio de otros firewall, lo que la aumenta. Es importante comprender que la implementación de un firewall –como el que actualmente tiene la empresa- no es suficiente para lograr la completa seguridad en una instalación ya que estos no abarcan todas las funciones necesarias, por ejemplo no pueden detectar un virus, no pueden detectar una intrusión interna, no previenen fallos en dispositivos de almacenamiento, etc.

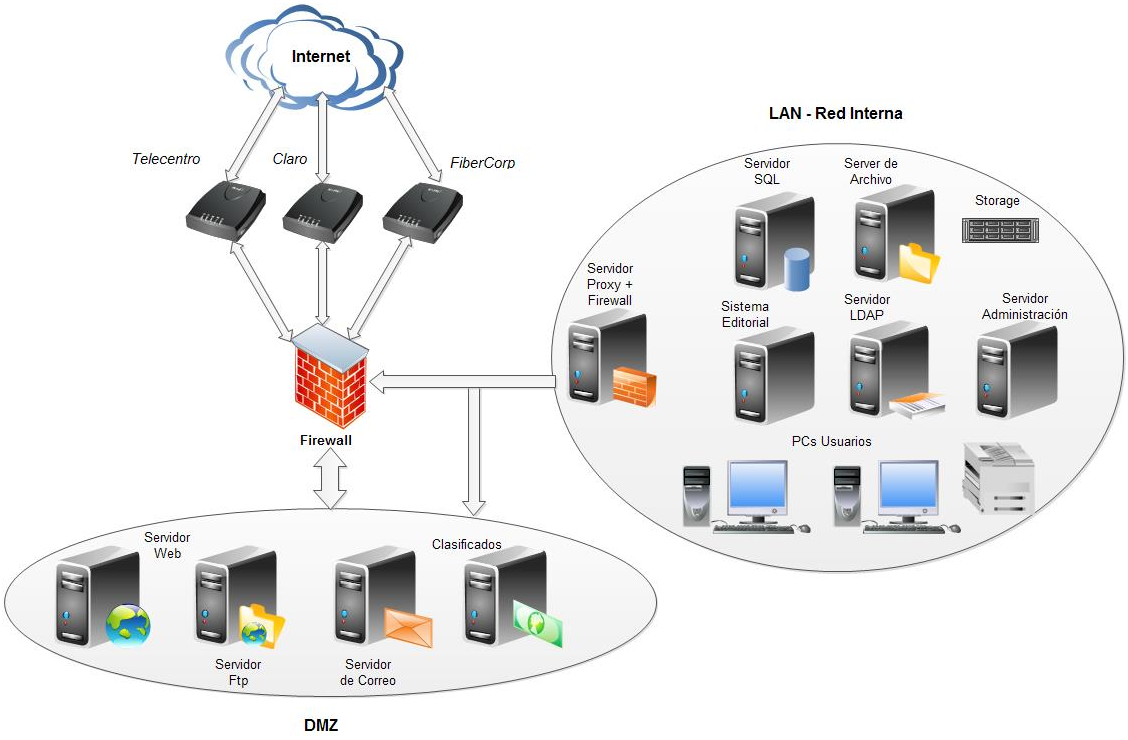


Figura 6: Esquema topológico de la red futura

7.6.2 DMZ

Un buen diseño de seguridad se da al separar los equipos, generalmente servidores, que tienen los diferentes servicios de internet como por ejemplo, los servidores de mail, Ftp, Web, y otros del resto de la red interna, donde no se desea ningún tipo de contacto desde el exterior (Internet). A esta zona, separada de la red interna, se la denomina DMZ (demilitarized zone) en referencia a la denominación de un sitio donde no se permite un conflicto militar.

La separación generalmente se hace por medio de un firewall con tres interfaces (interna, externa y DMZ) que permite el paso de los datos desde la red interna y desde la DMZ a Internet, desde Internet a la DMZ selectivamente y bloquea el tráfico desde Internet a la red interna. En algunos casos, el tráfico de internet pasa a la red interna, pero muy selectivamente.

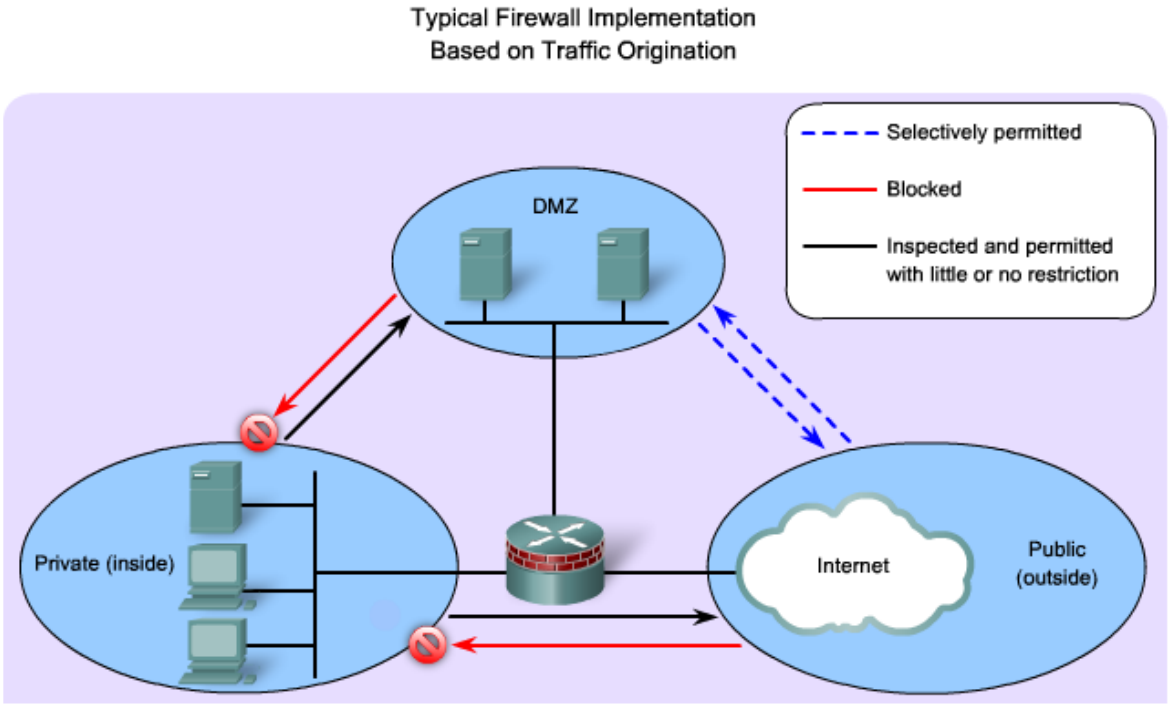


Figura 5: DMZ - Fuente CCNA Security (Cisco Certified)

7.6.3 VPN

Cuando se transmite información a través de una red pública como internet, esta pasa por diferentes dispositivos intermedios tales como routers, switches y equipos similares que la manipulan antes de que llegue a su destino. Durante todo este trayecto, la información está expuesta en varias oportunidades a ser interceptada y podría, entonces, ser alterada o cambiada. En la eventualidad de que esta información sea alterada, se convertiría en falsa y sería recibida como si viniera de una fuente confiable.

La Seguridad Informática se basa en asegurar:

Confidencialidad: Nadie más que las partes interesadas debería entender la información.

Integridad: Los datos contenidos no deben cambiar.

Autenticidad: Las partes que se comunican deben estar seguras de que están conectadas con la parte destinada.

Una VPN constituye una forma de asegurar principalmente la integridad, confidencialidad y autenticidad de la información que es enviada a través de redes públicas, extendiendo una red privada sobre una red pública como internet. Esta habilita a los host interesados para enviar y recibir datos a través de redes públicas o compartidas, como si ellos fueran parte integral de una red privada con todas sus funcionalidades, seguridad y políticas de gestión. La integridad, confidencialidad y autenticidad se logran entonces, estableciendo una conexión virtual punto a punto donde los datos viajan cifrados.

También es posible la utilización de conexiones dedicadas, que son líneas de telecomunicación provista generalmente por una compañía telefónica mediante un enlace de fibra óptica, y que se usan para interconectar dos lugares (punto a punto) o más (multipunto), está líneas son privadas por lo que, en principio, son seguras y no es necesario, por lo tanto, cifrar los datos, pero tienen un costo mayor que un enlace de internet.

7.6.4 Implementación de Firewalls UTM

Para poder implementar nuestra estrategia de seguridad en la red de la organización, se propone la compra e instalación de dispositivos capaces de implementar el resguardo deseado. Estos dispositivos son llamados Firewalls UTM (Unified Threat Management) por las siglas en inglés de gestión unificada de amenazas.

En un único de estos dispositivos de seguridad se pueden implementar simultáneamente: Firewalls, Proxy, VPN, Antivirus, IDS (detección de intrusos), IPS (prevención de intrusos), Antispam entre otras funciones.

Dada la carga actual de la organización en el uso de internet, y previendo un aumento del mismo, se realizó un estudio de mercado y se concluyó que las mejores opciones son el Sophos UTM SG230, o el Dell SonicWall 2600. Ambos equipo tienen características y un costo similar; están diseñados para ser usados en pequeñas y medianas organizaciones, aunque el firewall Sophos tiene una mayor capacidad en análisis de datos por segundo para la mayoría de las funciones (Firewall, VPN, IPS, Antivirus).

En los dos equipos las funciones se habilitan con la compra de la licencia correspondiente a cada función y por un lapso de tiempo limitado que varía de 1 a 3 años.

8. Logros, contratiempos y mejoras futuras

8.1 Logros

A raíz de este trabajo, se logró generar un informe que pudo ser expuesto a la gerencia de la empresa lo que dio lugar a la implementación de muchas de las medidas propuestas y a la compra e instalación de algunos dispositivos -Servidores, Firewall UTM y NAS- necesarios para mejorar la seguridad y la redundancia de la información, como ser:

- Incorporación de un servidor NAS de última generación (Lenovo Storage N3310), que se configuró como el dispositivo de almacenamiento principal de la empresa.
- Implementación de planes de backups automáticos de archivos y bases de datos. Control de los mismos en forma diaria por parte del personal que usa la información.
- Programación de réplicas automáticas de bases de datos del sistema ERP sobre servidores de backups internos y en la nube (Dropbox).
- Implementación de una política de cambio periódico de contraseñas (activando tiempo de caducidad) y robustez de las mismas (directiva de contraseña segura activa).
- Instalación de un circuito cerrado de televisión (CTTV) para las áreas sensibles como, por ejemplo, los accesos al Datacenter y a las áreas administrativas.
- Como parte de la seguridad física, también se llevó a cabo la incorporación de una cerradura biométrica –de acceso con huella digital o con tarjeta- para la entrada al Datacenter.
- Segmentación de la red interna LAN en tres segmentos (Redacción Gral., Administración y Producción) y creación de una zona DMZ con los servicios de Mail, FTP, Avisos Clasificados y Web, de esta forma se mejoró el control y la seguridad de acceso a los datos, lo que conllevó una mejora en el ancho de banda de las subredes.
- Compra e instalación de un firewall UTM Sophos SG230, usado para la ejecución de la DMZ y la configuración e implementación del uso de

VPN para el acceso remoto, dando seguridad a las conexiones externas.

- La protección de mails (antivirus y antispam) quedó a cargo del firewall Sophos.

8.2 Contratiempos

Todas las mejoras propuestas no pudieron ser implementadas, algunas por problemas financieros y otros por cuestión de tiempo y recursos. También nos hemos encontrado con algunos problemas al tratar de lograr las mejoras. La siguiente es una lista de lo que no se pudo realizar y de algunos inconvenientes.

- No se logró implementar –por el alto costo del mismo- un sistema de alta disponibilidad y tolerante a fallas como el propuesto con la compra “VMware vSphere” y sus módulos.
- Se advirtió una importante resistencia, por parte de los trabajadores, al cambio periódico de las contraseñas y a la complejidad que se les pide en ellas.
- Se recibieron quejas por la instalación de cámaras de seguridad.
- Se presentaron otros obstáculos entre los que se destacan la cuestión económica, la falta de tiempo por sobrecarga de tareas y la falta de personal capacitado en área de sistemas.

8.3 Mejoras Futuras

Para el futuro nos proponemos lograr:

- Conseguir la financiación para la compra e instalación de un sistema de alta disponibilidad y tolerante a fallas -VMware-.
- Incorporar la protección inalámbrica (WiFi) en el firewall Sophos (comprar la licencia).
- Mejorar la climatización del Datacenter, para lo que es necesario la instalación de un sistema de refrigeración con equipos de precisión (HVAC), en reemplazo de los equipos actuales de uso domiciliario.

- Incorporar un nuevo dispositivo de almacenamiento NAS (Lenovo Storage N3310), para agregarle redundancia al sistema de almacenamiento principal de la empresa.
- Mejorar la seguridad física de toda la planta. Ya se encuentra en proceso el análisis para la compra e instalación de un sistema de acceso por molinetes activados por huella digital para el personal permanente y por el uso de tarjeta RFID (del inglés Radio Frequency Identification) para las visitas.
- Instalación de más cámaras al circuito de CCTV (en portones de carga y descarga, depósitos, pasillos, etc.).

9. Conclusiones

Este trabajo se trató de un caso real dentro de una empresa periodística y, gracias al mismo, se ha logrado una mejora en todo lo relacionado a la seguridad de la información y a la continuidad operativa de los procesos críticos vinculados a la producción.

En particular, se ordenaron y se implementaron controles para diferentes tareas de mantenimiento informático ya existentes, se crearon protocolos que antes no existían, se planearon y se efectuaron salvaguardas para muchos de los procesos críticos, a la vez que se concientizó a los trabajadores y a la gerencia de la importancia de la seguridad de la información para garantizar la salida del diario. Igualmente consideramos que queda mucho por hacer y mejorar.

En definitiva, la empresa cuenta ahora con las herramientas y el conocimiento para poder enfrentar -con acciones adecuadas- un incidente, de forma de minimizar los inconvenientes y lograr la continuidad del negocio.

Bibliografía

- [1]Norma ISO/IEC 27001 – Sistemas de Gestión de la Seguridad de la Información
- [2]Norma ISO/IEC27002 –Sistemas de Gestión de la Seguridad de la Información–Código Buenas Prácticas
- [3]Norma ISO/IEC27005 – Gestión de Riesgo de la Seguridad de la Información.
- [4]Norma ISO/IEC31000
- [5]CCNA Security (Cisco Certified) versión 1.1 (archivo adobe pdf en español 589 páginas)
- [6]Windows Server 2008; instalación, configuración y administración. (María Pérez, Alfaomega Grupo Editor MX**)**
- [7]Check Point Software Technologies, Check Point Security Administrator R70/R71 TRAINING MANUAL Instructor's Edition, Primera Edición Julio de 2010. 280 paginas. ISBN 978-1-935862-00-0.
- [8]APC – Informe Técnico N° 82 – Seguridad Física en Instalaciones de Misión Crítica - Revisión 1.(por Suzzane Niles)
- [9]**10 STEPS TO DO IT YOURSELF CRAMM** http://www.itsmsolutions.com/newsletters/DITYvol2iss8.htm
- [10]**Herramienta de Evaluación de Riesgo-CRAMM** https://seguridadinformaticaufps.wikispaces.com/Herramienta+de+Evaluacion+de+Riesgo-CRAMM
- [11]**VMware vSphere -** http://www.vmware.com/ar/products/vsphere/
- [12]**VMware High Availabity -** http://www.vmware.com/ar/products/vsphere/features/high-availability.html
- [13]**VMware Fault Tolerance -** http://www.vmware.com/ar/products/vsphere/features/fault-tolerance.htmll
- [14]**IBM -Familia IBM Storwize – Dispositivos de almacenamiento**http://www-03.ibm.com/systems/ar/storage/storwize/

- [15]**¿Qué es un Firewall UTM?** http://www.uees.edu.sv/blogs/oscard/?p=611
- [16]**Dell SonicWall 2600** http://www.sonicwall.com/us/en/products/NSA-2600.html
- [17]**Sophos SG Series Appliances -** sophos-sg-series-appliances-brna.pdf https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-sg-series-appliances-brna.pdf?la=en

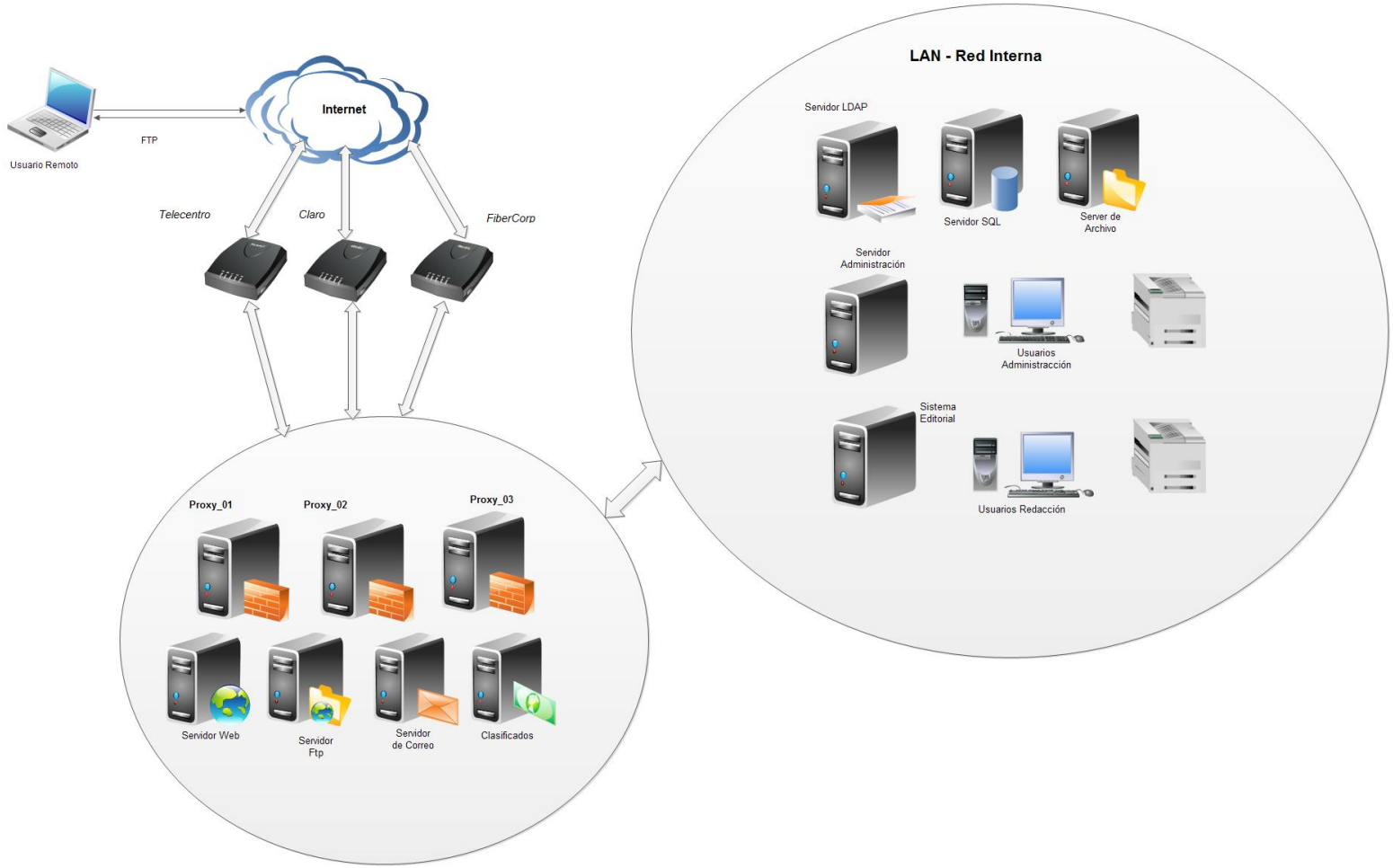
A. ANEXO

A.1. Composición del parque informático

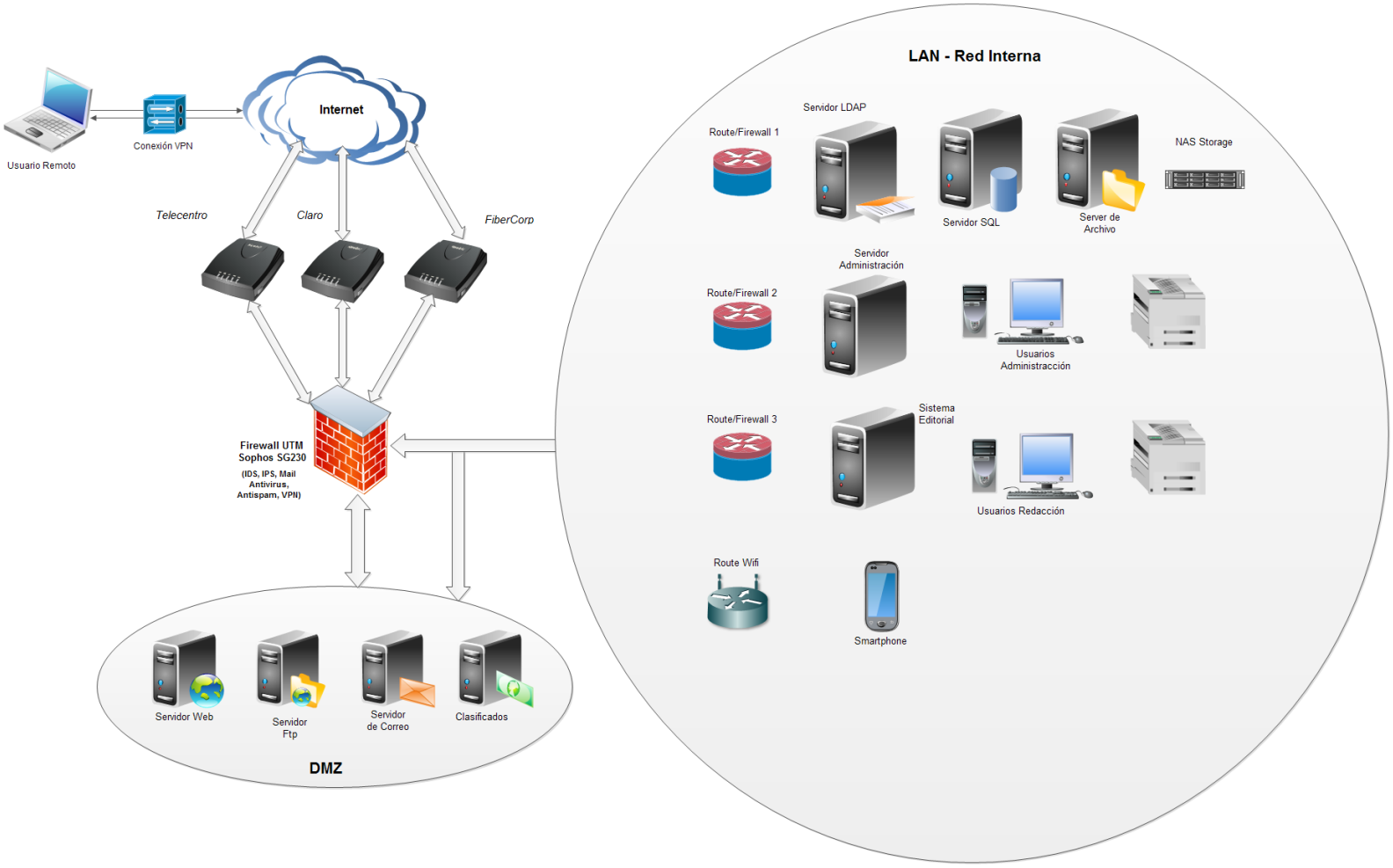
	PC	NAS
DataCenter	23	4

	PC	Impresora	TV
Fotografía	6	1	1
Fotomecánica	9		
Armado/Corre	8		
Armado	8	1	
Redacción	20	1	2
Espectáculos	10		2
Zonales	10	1	1
Web	9	1	2
Deportes	18		3
Sub. Sec.	1		
Sec. Gral.	1		1
Director	1		
AG. Quilmes	10		
Administración	10	2	
Gerencia	6	2	
Compras	8	1	
Expedición	2	1	
CTPs	9		
Rotativa	6		
Archivo	5	1	
Oficinas Varias	10		
Técnica	8		
TOTAL	198	12	12

A.2. Topología de la RED Anterior



A.3. Topología de la RED Actual



A.4. DataCenter

		Clasificados-2 (50.x)	Server Web Interno / HelpDesk	Server WEB-2	Server WEB-1
	Rack-1	Gabinete-1	Gabinete-2	Gabinete-3	Gabinete-4
	Router/Firewall-1				
	Switch-Internet (24Bocas)				
	Switch-1 (24Bocas)				
Rack Comunicación	Switch-2 (24Bocas)				
	Switch-3 (24Bocas)			NAS Levovo N3310	
Router- Claro	Switch-4 (24Bocas)	NAS 1,2,3	IMPREBA-SD1	LDAP Novell-1 / AD-1	Sever ERP/CRM Administración-1
Router-FiberCorp	Switch-5 (24Bocas)	Proxy / Mail	IMPREBA-SQL1	LDAP Novell-2 / AD-2	Sever ERP/CRM Administración-2
Router-Telecentro	Switch-6 (24Bocas)	Proxy / Mail	IMPREBA-SD2	Server-Partes1 (Producción)Linux	Server ERP/CRM-Quilmes
Router ADSL Fibertel	Switch-7 (24Bocas)	IMPREBA-AC1	IMPREBA-SQL2	Server-Partes2 (Producción)Linux	Server CCTV-1
Router ADSL Speedy	Switch-8 (24Bocas)	Serv_IDRemoto (Indesign)	Server EFE	DVR CCTV-2	Server AFP