MAESTRÍA EN REDES DE COMUNICACIÓN

CON ESPECIALIZACIÓN EN SEGURIDAD

MAESTRÍA PROFESIONAL

OPCIÓN DE TITULACIÓN: PROYECTO DE GRADUACIÓN

INFORME FINAL DEL PROYECTO DE GRADUACIÓN

PROPUESTA DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN PARA LA SOCIEDAD PANAMEÑA DE PRODUCTORES FONOGRÁFICOS (PRODUCE)

Asesor: ABDY MARTÍNEZ

Estudiante: ZELLIDETH E. HERNÁNDEZ

Número de Cédula: 8-748-2464

Cohorte: 18-01-2016

Aprobado por el Asesor:

_____

Panamá, 22 de Febrero de 2017.

Agradecimiento:

Las primeras palabras de agradecimiento son para Dios, por su bendición y la sabiduría otorgada para culminar este proyecto, sin Él nunca hubiera encontrado un norte a seguir; a mi Asesor Prof. Abdy Martínez, gracias a su apoyo, conocimientos y ayuda pude concluir con éxito este proyecto; a mi familia especialmente a querida Tía Madrina Agripina por alentarme a seguir hasta el final y estar pendiente en todo momento, a mis hijos Alexander y Alexandra mi motor de vida que con sus besos y abrazos me daban la energía necesaria para superarme cada día más.

¡Muchas gracias por todo su apoyo!

Contenido

I. FUNDAMENTOS

Sin importar la dimensión de la empresa, grande, mediana o pequeña, siempre debe ser prioridad resguardar la información, y evitar la interrupción de servicios y fallas críticas en la infraestructura.

Todos los días se desarrollan nuevas formas de afectar la seguridad de la información y vulnerar las estrategias de seguridad de cualquier organización; por esto es importante establecer un plan integral y un modelo de seguridad siguiendo las mejores prácticas.

Por esta razón, este proyecto busca establecer una Propuesta de un Plan de Seguridad de la Información para la Sociedad Panameña de Productores Fonográficos (PRODUCE).

Dicha Sociedad en la actualidad no cuenta con políticas, procesos, procedimientos, controles, hardware ni software adecuados y sobre todo la cultura organizacional adecuada para velar por la protección de la información, estando expuestas a una amplia gama de amenazas y vulnerabilidades.

Adicional se busca crear conciencia, educar y lograr la aprobación de parte de la Dirección General del Plan de Seguridad de la Información; buscando siempre mantener la confidencialidad, integridad y disponibilidad de los datos.

A. Generalidades de la Empresa

El Proyecto se va a realizar en la Sociedad Panameña de Productores Fonográficos (PRODUCE). Esta es una Sociedad sin fines de lucro, con personería jurídica otorgada por el Ministerio de Gobierno. Con una licencia de Operaciones otorgada por la Dirección General de Derecho de Autor del Ministerio de Comercio e Industria, en enero del año 2007.

PRODUCE es una Sociedad reconocida a nivel Internacional por la OMPI (Organización Mundial de Propiedad Intelectual), y por ende la Sociedad de Gestión Colectiva representa a titulares internacionales a fin dar Cumplimiento al Principio de Trato Nacional, previstos en los Convenios y Tratados Internacionales, relativos a la Propiedad Intelectual.

PRODUCE cuenta con el apoyo de la Federación Internacional de la Industria Discográfica (IFPI), cuya sede se encuentra en Europa Londres y se cuenta con una Sede Regional para América Latina en Miami –USA.

PRODUCE está obligada a representar a todo productor sin distinción de género musical. Se han firmado convenios con diferentes grupos gremiales en Panamá, los cuales han aceptado y entendido el pago de los Derechos de Comunicación Pública y Reproducción de Productores Fonográficos e Intérpretes, algunos de estos gremios son APATEL, ARAP, APR y la Cámara de Comercio.

B. Derechos que Recauda PRODUCE

Actualmente son leyes de la República de Panamá, los dos (2) instrumentos internacionales base de la protección de los Productores Fonográficos y de los Artistas: la Convención de Roma de 26 de octubre de 1961 (Panamá forma parte de la Convención desde el 2 de septiembre de 1983) y el Tratado WPPT (ratificado por Panamá en 1998). Las normas de protección mínimas adoptadas en la Convención de Roma de 1961 se encuentran contenidas en la Ley de Derecho de Autor de la República de Panamá.

¿Qué establecen ambos instrumentos internacionales? Establecen que el Estado panameño debe velar por los derechos de Titulares de Derechos Conexos al Derecho de Autor, siendo éstos los

Artistas, los Productores Fonográficos y los Organismos de Radiodifusión. Una canción tiene varios titulares de derechos de propiedad intelectual:

- sobre la letra y música: los autores y compositores,
- sobre las interpretaciones: los artistas y músicos. Y, si esa canción fue fijada o grabada
- sobre las grabaciones o fijaciones de esas interpretaciones: los productores discográficos.

Todos y cada uno tienen derecho a recibir regalías por la utilización fuera de los límites previstos en la Ley de Derecho de Autor No. 64 de 10 de octubre de 2012. El artículo 67 de la Ley de Derecho de Autor establecen los límites que tiene estos titulares; se mencionan, cuando la música es disfrutada en un círculo familiar; cuando la comunicación pública es efectuada en el curso de un acto religioso y un acto oficial; las verificadas en los centros de enseñanza, etc. Así tenemos que todo lo que está fuera de éstas limitaciones que son "numerus clausus" dentro de la ley, deben pagar u obtener las respectivas autorizaciones de los titulares.

1. Comunicación Pública

Los derechos de Comunicación Pública o el Derecho que tiene un titular de recibir regalías cada vez que alguna persona fuera de los límites previstos en la ley de Derecho de Autor, pone al alcance o a disposición de un público a través de cualquier medio (análogo o digital) las obras, producciones e interpretaciones, sin haber una previa distribución de la obra entre ese público. Siendo así desde estaciones de radio, televisión, y locales comerciales que cuentan con receptores de sonido y/o imagen están obligados por ley a pagar estas regalías. A nivel mundial este derecho lo ejercen los autores desde hace siglos a través del sistema de gestión colectiva (El Convenio de Berna, que protege los derechos de los autores data de 1886, con posteriores revisiones). Los Productores de Fonogramas y Artistas lo ejercen a través de su sistema de Gestión Colectiva desde hace unos 30 años. A nivel mundial existen en los 5 continentes países con Sociedades de Autores,

Artistas y Productores. Cada grupo Autores y Derechos Conexos cobran sus respectivas regalías. En Panamá con la creación de PRODUCE y PANAIE se cierra un círculo (la representación de Derechos Conexos y sus cobros por la comunicación pública).

2. La Licencia de Reproducción

Los Productores a nivel mundial tienen un derecho exclusivo llamado el derecho de reproducción. Nadie puede reproducir una grabación (salvo las excepciones que también prevé la Ley) sin contar con la autorización de la compañía discográfica; el acto de violación por no contar con estas autorizaciones es conocido vulgarmente como PIRATERÍA, que se sanciona con pena de prisión de 4 a 6 años, de acuerdo al Código Penal de Panamá. Así tenemos en resumen que las organizaciones de casas disqueras licencian por:

- la Comunicación Pública de los Fonogramas e Interpretaciones;
- la Reproducción de dicho fonograma siempre y cuando sea para comunicarlo al público posteriormente (no se licencia para vender o distribuir piratería)
- y cualquier otro derecho previsto en la Ley a favor de éstos titulares

Junta Directiva Actual de PRODUCE está conformada por:

- Ricardo Ramírez – Presidente – Contraxeñas
- Jorge Escobar – Vicepresidente – Disco Tamayo
- Carmen de Alfanno – Vocal – Representante de SONY MUSIC
- Elsa Vásquez – Tesorera – Representante de UNIVERSAL MUSIC
- Ana Tovar – Secretaria – Any Tovar

La Sociedad Panameña de Productores Fonográficos (PRODUCE), está localizada en Vía España Torre del Banco Delta, piso 5 oficina 505.

Sus redes sociales:

- Página web: producepanama.org
- Twitter:@producepanama.org
- Facebook: produce
- Instagram: produce_panama.

II. OBJETIVOS

A. Objetivo General

Elaborar una Propuesta de un Plan Estratégico de Seguridad de la Información siguiendo las mejores prácticas y estándares internacionales de seguridad, que apoyen a mejorar la seguridad de la información que se almacena, transita y se procesa, sin afectar las operaciones cotidianas de la Sociedad Panameña de Productores Fonográficos (PRODUCE).

B. Objetivos Específicos

- Controlar, prevenir y/o mitigar los riesgos de seguridad de la información, identificando las vulnerabilidades y amenazas más críticas y proponiendo su remediación.
- Recomendar el establecimiento de políticas, normativas y procedimientos básicos que permitan resguardar y proteger la información de la Sociedad.
- Definir un Plan de Difusión, Sensibilización y Capacitación de buenas prácticas asociadas a la seguridad de la información de la Sociedad.
- Identificar los recursos necesarios para la implementación de las medidas de seguridad y sus diferentes presupuestos aproximados.

III. ALCANCE DEL PROYECTO

El alcance del proyecto involucra la elaboración de una Propuesta de Plan Estratégico de Seguridad de la Información para la Sociedad Panameña de Productores Fonográficos (PRODUCE).

Este plan busca definir un norte a PRODUCE para remediar los hallazgos encontrados en la auditoría realizada y definir los controles necesarios a aplicar para la protección de los datos. Lo más importante que intenta alcanzar este proyecto es crear conciencia ante los directivos de la Sociedad de la importación de salvaguardar toda la información de sus Socios, manteniendo como ejes principales la confidencialidad, integridad y disponibilidad de los datos.

Se presentará una propuesta de mejoras que requieren ser realizadas dentro de un modelo de seguridad de la información, no se efectuará una implementación, ya que esta depende de un presupuesto con que el que no se cuenta en este momento (y con el que esperamos contar, luego de presentar los hallazgos en este proyecto). Se desarrolló en un lenguaje claro, que pueda ser comprendido por todos los que tengan acceso al documento.

Para el desarrollo del proyecto se utilizará como guía principal la norma ISO 27001:2013, "que es una norma para los Sistemas Gestión de la Seguridad de la Información que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos".[1]

IV. MARCO TEÓRICO

Debido a la evolución permanente de las tecnologías de la información y las comunicaciones que demandan un mayor esfuerzo para garantizar la seguridad, a las constantes amenazas que hoy en día atentan contra la seguridad de la información que cada vez son más especializadas, complejas

[1] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001

y avanzadas, y a la normatividad vigente que regula y exige una mayor protección y privacidad de los datos sensibles, personales, comerciales y financieros de las personas, las organizaciones deben contar con un modelo o Sistema de Gestión de Seguridad de la Información basado en estándares de seguridad reconocidos a nivel mundial, con el propósito de poder establecer y mantener un gobierno de seguridad alineado a las necesidades y objetivos estratégicos del negocio, compuesto por una estructura organizacional con roles y responsabilidades y un conjunto coherente de políticas, procesos y procedimientos, que le permiten gestionar de manera adecuada los riesgos que puedan atentar contra la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio de la seguridad de la información.

Para lograr una adecuada gestión de la información es indispensable que las organizaciones establezcan una metodología estructurada, clara y rigurosa para la valoración y tratamiento de los riesgos de seguridad; conociendo el estado real de la seguridad de los activos de información; identificar y valorar las amenazas que puedan comprometer la seguridad de la información y determinar los mecanismos y medidas de seguridad a implementar para minimizar el impacto en caso de las posibles pérdidas de confiabilidad, integridad y disponibilidad de la información.

A. Levantamiento

Una red de ordenadores, o de comunicaciones de datos, es un conjunto de equipos informáticos y software conectados entre sí; los cuales por medio de dispositivos físicos envían y reciben impulsos eléctricos, los cuales transportan datos, cuya finalidad es compartir información, recursos y ofrecer servicios. Su principal finalidad es compartir los recursos y la información de formal, segura, confiable y que se encuentre a la disponibilidad de los usuarios, aumentando la velocidad de transmisión de los datos y reducir el costo.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI, esta estructura divide cada red en siete capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro capas.

Las redes están compuestas por: hardware, software, dispositivos del usuario final, servidores, etc. Se pueden dividir por su alcance, tipo de conexión y tecnología.

Es necesario utilizar diferentes tipos de dispositivos para una red alámbrica e inalámbrica en las empresas en crecimiento o PYMES.

A continuación, mostramos una tabla con los principales dispositivos que se requieren en una red, su uso, finalidad y desafíos.

Servicio	Dispositivo Principal	Uso Principal	Beneficios	Desafíos
Red de área Local (LAN)	Conmutadores	Conectar servidores, dispositivos y PC	Conectividad LAN de alta velocidad	Cablear la LAN
Conectividad alámbrica segura en la LAN	Puntos de acceso alámbricos	Conectar dispositivos habilitados de manera inalámbricas	Movilidad del Cliente	Seguridad, velocidad de transmisión
Conexión segura a Internet	Firewall	Proporcionar acceso de entrada y salida a Internet	Conectarse con Socios y Proveedores	Seguridad

Tabla 1. Servicios de Infraestructura[2]

[2] technet.microsoft.com/es-es/library/dd568932.aspx

B. Evaluación y Análisis

Sistema de Gestión de la Seguridad de la Información abreviada SGSI "es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001"[3]

El ciclo de mejora continua, también conocido como ciclo PDCA (del inglés Plan-Do-Check-Act) o PHVA (Planificar-Hacer-Verificar-Actuar) o Ciclo de Deming por ser Edwards Deming su creador, es uno de los sistemas más usados para la implementación de un sistema de mejora continua, el cual establece cuatro pasos o fases esenciales que de forma sistemática las organizaciones deben llevar a cabo para lograr la mejora continua de sus sistemas de gestión; en su forma gráfica.

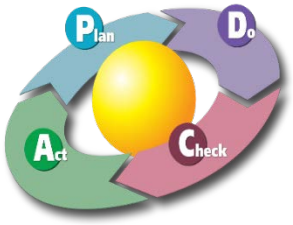


Figura 1. Círculo de Deming

De acuerdo a la norma NTC-ISO-IEC 27001:2013, un Sistema de Gestión de Seguridad de la Información tiene por finalidad preservar la confidencialidad, integridad y disponibilidad de la información, a través de la aplicación de un proceso de gestión del riesgo.[4]

Un Sistema de Gestión de Seguridad de la Información, les permite a las organizaciones gestionar de manera efectiva los riesgos asociados a la seguridad sobre sus activos de información mediante la identificación de las amenazas que puedan llegar a comprometer la seguridad de sus activos de

[3] Tomando de wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n
[4] NTC-ISO-IEC 27001:2013, Capitulo Introducción

información, lo cual, genera confianza en sus partes interesadas debido a que demuestra que los riesgos de la organización son debidamente gestionados.

La información es el conjunto de datos organizados en poder de una entidad que posean valor para la misma, sin importar la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información en una organización, es un proceso de mejora continua que demanda la participación activa de toda la organización y busca preservar, entre otros, los siguientes principios de la información:

- La confidencialidad, asegurando que solo las personas debidamente autorizadas tengan acceso a la información.
- La disponibilidad, asegurando que la información esté totalmente disponible para las personas debidamente autorizadas cuando ellos la requieran.
- La integridad, asegurando que la información no sea modificada sin la debida autorización.
- La autenticidad, con el propósito de garantizar la identidad de la persona que genera la información. La autenticidad de la información, es la capacidad de asegurar que el emisor de la información es quien dice ser y no un tercero que esté intentando suplantarlo.
- El no repudio, con el propósito de conocer exactamente quienes son los actores que participan en una transacción o una comunicación y no puedan negarlo en ningún momento. El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje.

- La trazabilidad, con el objetivo de poder monitorear o rastrear cualquier operación que se realiza sobre la información desde su mismo origen.

La seguridad de la información dentro de las organizaciones, depende del nivel de protección y seguridad de sus activos de información, por tanto, es fundamental la implementación de medidas y controles de seguridad adecuados, y el permanente monitoreo, revisión y mejora de los mismos de manera proactiva con el objetivo de garantizar su efectividad.

C. Diseño de Plan de Seguridad

"El Plan de Seguridad Informática es la expresión gráfica del Sistema de Seguridad Informática diseñado y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una Entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo".[5]

El riesgo a un ciberataque, hoy en día, es real. Les ocurre a grandes y pequeñas empresas e incluso a algunas de las organizaciones que parecen más seguras. Por lo tanto, un plan de seguridad informática no es algo de lo que deberíamos dudar de tener.

Un plan de seguridad de la información permite entender donde puedes tener vulnerabilidades en los sistemas informáticos, para una vez detectadas, tomar las medidas necesarias para prevenir esos problemas.

[5] http://files.sld.cu/gau/files/2009/03/plan_seguridad.pdf

El Plan de Seguridad debe ser capaz de ayudar a proteger los datos y los sistemas críticos del negocio, asegurando además que se ajuste a la legislación vigente y a la Ley de Protección de Datos.

El plan de seguridad debe de tener varios pasos que se deben dejar por escrito, entre los que podemos mencionar:

- Identificación: Para proteger la organización, lo primero es conocer todo lo que vale la pena proteger; todo el conjunto de los activos de la organización, el personal, el hardware, software, sistemas y datos que componen el sistema informático (programas informáticos, servidores y servicios externos como alojamiento web).
- Evaluación de riesgos: Conocer qué es lo que podría poner en peligro los activos ya determinados. Por ejemplo, los virus informáticos, hackers, daños físicos o errores de los empleados. Es importante conocer el tipo y el alcance del daño que podría ser causado en cada caso. (si el servidor se pone fuera de línea, ¿la empresa podría seguir funcionando?
- Prioriza tu protección IT: Ya evaluado el daño potencial de cada amenaza y la probabilidad de que se produzca, podemos decidir qué amenazas son las más importantes para empezar a proteger. (la protección del servidor es más importante que la protección de los equipos individuales).
- Tomar las precauciones adecuadas: Decidir cuáles son los pasos que se debe tomar para protegerte contra los riesgos que se han identificado en el plan de seguridad informática, y asegura que el negocio va a seguir siendo capaz de operar si se produjera algún incidente. (restringir el acceso al servidor o instalar un firewall de hardware). El plan de recuperación de desastres debe explicar qué hacer si ocurre una crisis.

V. METODOLOGIA

El Proyecto está dividido en diferentes fases: Levantamiento de la Información de la Red Existente, Evaluación y Análisis de las Información recopilada y Diseño de un Plan de Seguridad de la Información, que incluye primordialmente la remediación de los hallazgos más críticos. En estas tres etapas consideramos los siguientes 5 tópicos:

- Networking
- Servidores
- Aplicaciones utilizadas
- Personal Administrativo
- Documentación

La primera parte es el Levantamiento de la Información de la red existente. Todos los aspectos relacionados con la concepción del Plan de Seguridad de la Información, especialmente las necesidades de protección, mostrar la red actual de la empresa con las respectivas aplicaciones que se manejan, concientizar y capacitar al personal en uso de los recursos informáticos y la documentación que no es más que un texto redactado con la finalidad de que quede por escrito todo lo realizado

La segunda parte es la Evaluación y Análisis; en el cual se analizarán la información recabada en base a las mejores prácticas y recomendaciones en temas de seguridad de la información y la gestión de los riesgos sobre los sistemas informáticos, los controles necesarios a implementar, políticas, procesos, procedimientos, mejorando cuanto fuera necesario para asegurar que se cumplan los objetivos de seguridad.

La tercera parte es Diseño en esta parte se entrega la Propuesta del Plan de Seguridad de la Información finalizada, donde buscamos listar las recomendaciones de acciones para remediar los hallazgos encontrados y resaltar la importancia de que exista un Sistema de Gestión de Seguridad de la Información.

Presentamos un cronograma del desarrollo de las actividades a realizar para el desarrollo eficiente de esta propuesta.

PROPUESTA DE PLAN DE SEGURIDAD DE LA INFORMACION PARA LA SOCIEDAD PANAMEÑA DE PRODUCTORES FONOGRAFICOS

CRONOGRAMAS DE ACTIVIDADES

		SEMANAS														
ACTIVIDADES		1	2	3	4	6	7	8	9	10	11	12	13	14	15	16
LEVANTAMIENTO																
1	NETWORKING															
2	SERVIDORES															
3	APLICACIONES															
4	PERSONAL ADMINSTRATIVO															
4.1	DIRECCION GENERAL															
4.2	CONTABILIDAD															
4.3	COBROS															
4.4	LEGAL															
4.5	MERCADEO															
4.6	IT															
5	DOCUMENTACION															
EVALUACION/ ANALISIS																
1	NETWORKING															
2	SERVIDORES															
3	APLICACIONES															
4	PERSONAL ADMINSTRATIVO															
4.1	DIRECCION GENERAL															
4.2	CONTABILIDAD															
4.3	COBROS															
4.4	LEGAL															
4.5	MERCADEO															
4.6	IT															
5	DOCUMENTACION															
DISEÑO DEL PLAN DE SEGURIDAD																
1	NETWORKING															
2	SERVIDORES															
3	APLICACIONES															
4	PERSONAL ADMINSTRATIVO															
4.1	DIRECCION GENERAL															
4.2	CONTABILIDAD															
4.3	COBROS															
4.4	LEGAL															
4.5	MERCADEO															
4.6	IT															
5	DOCUMENTACION															

Tabla 2. Cronograma del Proyecto

VI. RESULTADOS Y ANÁLISIS DE RESULTADOS

A. Resultados

Se describirá de manera detallada la infraestructura tecnológica de la Sociedad, redes instaladas, aplicaciones propias si existen, características de los procesos y del personal, la estructura del local y la estructura eléctrica.

1. Análisis físico de las instalaciones

- Condiciones ambientales: las oficinas se mantienen a una temperatura de 23°C.
- Espacio: las oficinas miden 100 mts 2, ubicadas en Vía España Torre Delta, piso 5 oficina 503, calle Elvira Méndez, enfrente de la estación del Metro Iglesia del Carmen.
- Red eléctrica: IP de 100A dos polos, panel de distribución de 20 circuitos 20A por circuitos dos fases, cantidad de tomas corrientes existentes 16 toma corrientes sencillos 110 voltios, 4 tomas corrientes 220 voltios dos polos, cuatro interruptores sencillos de 15A, 10 lámparas de 3 x 32 watts.

La siguiente imagen muestra un esquema de la distribución de la oficina

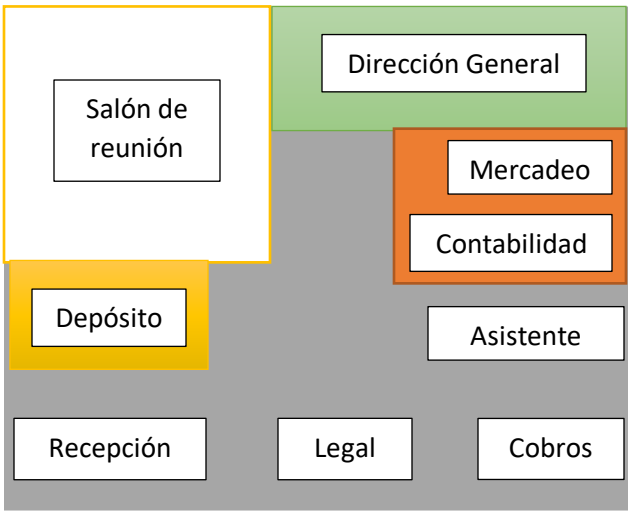


Figura 2. Distribución Física de la Oficina

2. Instalaciones Generales

- El cableado es el necesario para conectar el ADSL del proveedor con el router inalámbrico.

  Hay dos conexiones al router inalámbrico que son: PC de Contabilidad y PC de Cobros.

- La PC de la Dirección General se conecta directo a ADSL del proveedor.
- Las laptops se conectan vía inalámbrico al router.
- El punto de acceso Wireless está ubicado cerca de la entrada en el puesto Cobros.

El siguiente cuadro muestra la distribución de la red actual.

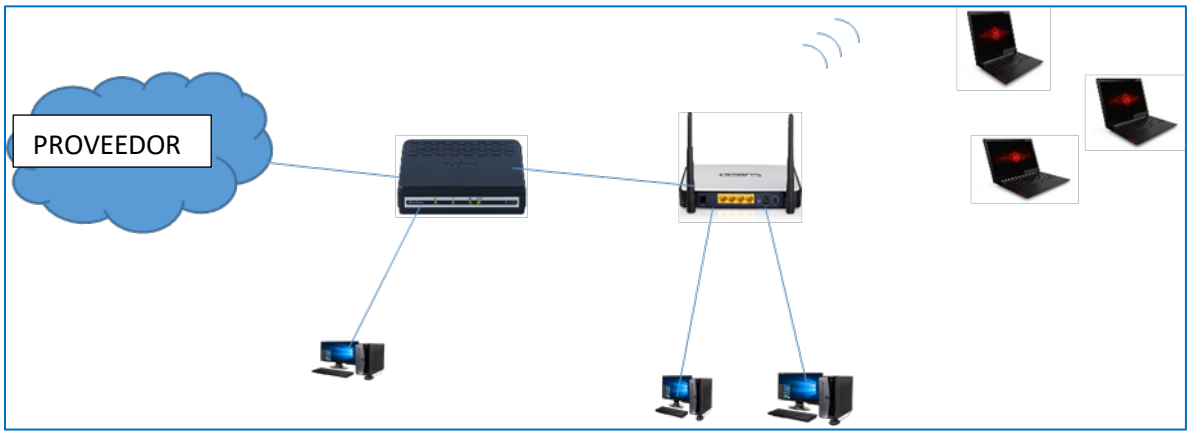


Figura 3. Diagrama de Red Actual

3. Análisis Hardware y Software

a) Inventario Hardware y Software Servidores, Equipos de Redes, Impresoras y Computadores Personales

Modelo	Nombre del Equipo	IP	Versión del SO
Dell	Dirección General	192.168.0.101	Windows 10 Pro, Office 2013 PRO, RAM 4.00 GB, Disco Duro 1 TB, Intel Core i5-4570 CPU 3.20 GHz; SO de 64 bits

Acer Aspire X	Contabilidad	192.168.0.103	Windows 7 PRO, Office 2010 Estudiante, RAM 4.00 GB, Disco Duro 1 TB; SO 64 Bits; Intel Core i3-2120 2.80 GHz; Sage 50 Acounting 2015 como servidor y usuario admin
Computadora de escritorio	Recaudación	192.168.0.124	Windows 10 Home Single, Microsoft Office Hogar y Empresa 2010, RAM 4.00, Intel Core i3 2.80 GHz, Disco Duro 1TB, Sage 50 Acounting 2015 como estación de trabajo
Laptop	Legal	192.168.0.107	Windows 7 starter Pentium Dual-Core CPU T4500 2.3 GHz, RAM 2.00GB So de 32 bits; Disco Duro de 500 GB; Office 2010 estudiante
Laptop	Asistente	192.168.0.105	Windows 7 starter Pentium Dual-Core CPU T4500 2.3 GHz, RAM 2.00GB So de 32 bits; Disco Duro de 500 GB; Office 2010 estudiante
Laptop	Mercadeo	192.168.0.109	Windows 7 starter Pentium Dual-Core CPU T4500 2.3 GHz, RAM 2.00GB So de 32 bits; Disco Duro de 500 GB; office 2010 estudiante
Canon Pixma iP2810	Impresora Sencilla		Pixma iP2810

Canon 250	Impresora Multifuncional		
Antivirus			Kaspersky 2015
Modem del Proveedor			8 Megas Internet
Linksys N600	Router Inalámbrico		Protocolo 802.11G, WPA2-Personal, Banda Ancha de 2.4 GHz, Cifrado AES
APC by Schneider Electric (UPS)			UPS 550
Central Telefónica PANASONIC	Ky-TES824		Advance Hybrid System
Epson LX-350	Impresora para cheques		
Red	Topología Lineal		
My Passport	Disco Externo		No cifrada

b) Respaldos

- Respaldos: Se realiza respaldo 2 veces por semana solo de la información de contabilidad, en un disco duro externo.

c) Observaciones sobre buenas prácticas

- Todas las máquinas cuentan con sus licencias y/o software legales

4. Aplicaciones

a) Página web

Contamos con una página Web cuyo dominio es producepanama.org adquirido con una compañía Panameña ICAMOS y el hosting esta un servidor de la compañía GoDaddy. No se ofrece ninguna medida de seguridad ni política de respaldo en caso de problemas; no se han registrado problemas hasta el momento.

b) Mail

Todos los empleados tienen una cuenta de mail, y todos los empleados necesitan de este servicio por ser la vía de comunicación entre personal y clientes. Este medio se utiliza para enviar todo tipo de información.

Las altas y bajas de los usuarios como los cambio a de contraseña son manejados por el departamento de informática.

Se muestra a través del siguiente cuadro el estado actual de la Red y Políticas de Seguridad de la Sociedad.

Networking	**Análisis Físico**
	No ha control de utilización de equipos de red
	No hay propiedad de recuperación de equipos
	Se desconoce alcanze de la señal Wifi
	Se desconoce si hay un sistema de encriptación entre servidores de correo electrónico
	No hay cambio periodico de contraseñas
	No se Registra las actividades de los usuarios en la red
	No hay revisión periodida de la red
	Cableado casi nulo
	No existen puentos de red
	No hay swicth
	No exiten VLAN
	No es una red administrada
	No exiten controles de acceso a oficinas y equipos de redes
Servidores	No cuentan con servidores
Aplicaciones	**Instalaciones generales (Hardware, Software)**
	No hay backup automatico
	No se lleva un control de programas instalados
	No hay programado un matenimiento para equipos
	Las aplicaciones se actualizan de forma automatica sin una prueba previa
	Estipular un tiempo de vida para equipos
Personal Administrativo	Todos tienen acceso a todas las máquinas
	No hay restricciones por uso de internet
	No estan cifrados o contraseña los dispositivos de almacenamientos externos
	No se cuenta con Firewall
Documentación	No se cuentan con politicas de seguridad
	No hay un sistema de documentación de documentos
	No se realiza una revisón previa par averificar afectaciones por actualización o parches
	No se cuenta con un manual de crisis ante falla y continuidad operacional
	No hay una estadistica de las tasas de errores y trasmisión

Tabla 3. Estructura de Red y Políticas de Seguridad

B. Análisis de Resultados

Ya realizado el análisis General de la Sociedad y conociendo de una forma más detallada el sistema informático actual, cuáles son los bienes más importantes para la Gestión de la Sociedad, consideramos que es necesario prestar especial atención a los siguientes puntos.

1. **Debilidades:** No existe una red administrada y la topología es lineal.

   Efectos: Ente los que podemos mencionar:

- ✓ Si un usuario desconecta su computadora de la red, o hay alguna falla en la misma como una rotura de cable, la red deja de funcionar.
- ✓ Las computadoras de la red no regeneran las señales, sino que se transmiten o son generadas por el cable y ambas resistencias en los extremos.
- ✓ En esta topología el mantenimiento a través del tiempo que hay que hacer es muy alto
- ✓ La velocidad en esta conexión de red es muy baja.

2. **Debilidades:** No se cuenta con un Servidor de aplicaciones

   Efectos: No se podrá acelerar el rendimiento de aplicaciones, optimizar cargas de trabajo o simplificar sistemas administrativos dentro de la empresa.

3. **Debilidades:** Las máquinas de la empresa disponen de disqueteras y lectoras de CD, aunque el 90% de los usuarios no las necesitan. Estos dispositivos están habilitados y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos.

   Efectos: Debido a que cualquier usuario puede introducir un USB o un CD con virus o intentar bootear desde estos dispositivos, esto implica un gran riesgo a la integridad del equipo y sus datos, y existe posible fuga de información.

4. **Debilidades:** No conocer la cobertura de la señal WiFi, y la red en la Empresa es mayormente inalámbrica.

   Efectos: Propagación de la señal a lugares no deseados; son menos eficientes, menos estables y menos segura; una red inalámbrica es más lenta.

5. **Debilidades**: Los usuarios deben realizar tareas de mantenimiento, como actualizar el antivirus, hacer copias de respaldo de sus datos, desfragmentar el disco, modificar y proteger sus password, borrar archivos temporales, entre otras.

Efectos: Estas son tareas que revisten gran importancia en el funcionamiento de los equipos de los puestos de trabajo, y una falla en su realización puede generar el mal funcionamiento de los mismos.

6. **Debilidades**: No se documentan los cambios que se realizan en la configuración de los equipos, ni la fecha de estas modificaciones

   Efectos: Al no tener documentación actualizada de los cambios realizados, se dificulta conocer la configuración exacta y actual de cada equipo, y de esta forma se obstaculiza la tarea del mantenimiento.

7. **Debilidades:** No hay ningún procedimiento formal para la realización ni la recuperación de los backups de los datos almacenados en los dispositivos portátiles de la empresa.

   Efectos: Las copias de respaldo son el principal método de recuperación de datos del que dispone la organización y la ausencia de procedimientos para su implementación puede generar errores en el momento de un incidente.

8. **Debilidades:** No poseen un plan de monitorización general de la red.

   Efectos: Al no contar con un plan organizado de monitorización, puede ocurrir que baje la performance del sistema debido a cuellos de botella en los recursos.

9. **Debilidades:** No hay un buen soporte de documentación en el centro de cómputos.

   Efectos: Al no poseer un buen soporte, la información puede ser incorrecta, inconsistente o desactualizada, lo que genera incertidumbre y dificulta la administración de incidentes**.**

10. **Debilidades:** No hay desarrollados planes de seguridad, procedimientos formales, ni demás manuales o documentos de soporte para la gestión de la seguridad en la red informática.

Efectos: Al no poseer un buen soporte, la información puede ser incorrecta, inconsistente o desactualizada, lo que genera incertidumbre en el momento de llevar a cabo procedimientos o procesos, lo que dificulta la administración general.

11. **Debilidades:** No hay ninguna medida tomada para que un usuario pueda proteger sus datos

    Efectos: Algún usuario puede acceder a datos de otro usuario que no deberían ser divulgados.

12. **Debilidades**: No se asocia una cuenta de correo a un equipo específico.

    Efectos: Un usuario, conociendo el nombre de cuenta y la contraseña de la cuenta de correo de otro usuario, puede configurarla en su máquina y así enviar y leer mensajes ajenos.

13. **Debilidades**: Los empleados no usan el mail solamente para funciones laborales, sino también con fines personales. Actualmente no se controla el envío, pueden usarlo para cualquier fin. No se hace ningún control de que los usuarios se suscriban a listas de correo, no hay prohibiciones en este sentido.

    Efectos: Al utilizarse el servicio de mail indiscriminadamente se puede bajar la performance de la futura red y se incrementa el riesgo de infección con virus.

14. **Debilidades**: No se implementa un sistema de prioridades de mail.

    Efectos: Podrían mejorarse el envío de los mails a destinos como fábricas, bancos, y otros que merezcan mayor consideración.

15. **Debilidades**: No se generan copias de seguridad de los mensajes.

    Efectos: En el caso de una contingencia con el servidor de Internet, los usuarios perderían los mails que no hayan leído hasta el momento del incidente.

16. **Debilidades:** No se utilizan firmas digitales ni encriptación en el correo electrónico a nivel gerencial.

Efectos: Sin la utilización de firma digital se puede correr el riesgo de ataques de ingeniería social.

17. **Debilidades**: Los usuarios son los responsables de actualizar sus propios antivirus.

    Efectos: Al no tener implantada una conciencia de seguridad, los usuarios no actualizan las listas de virus.

18. **Debilidades:** No hay procedimientos formales a seguir en caso de infección de virus.

    Efectos: Al no utilizar un procedimiento como guía, puede ocurrir que el virus no sea eliminado completamente del equipo y se contagie a través de la red interna, además de la posibilidad de pérdida de datos en los equipos infectados.

19. **Debilidades:** No se implementa ningún régimen de separación de tareas ni tampoco un sistema de rotación de personal.

    Efectos: Si un usuario tiene la capacidad (o los permisos) para realizar una tarea completa, pueden cometerse errores o fraude, sin que la irregularidad sea advertida. Al no haber una rotación de personal, es más difícil controlar la productividad del empleado, evitar posibles fraudes en el desempeño de sus funciones, así como el reemplazo del empleado en caso de su ausencia.

20. **Debilidades**: El archivo que contiene los datos de los empleados y socios de la empresa se encuentra almacenado en una PC, en texto plano, sin ningún control de acceso.

    Efectos: Ante el acceso indebido a datos de la PC, se divulgarían los datos de los empleados y socios de la empresa.

21. **Debilidades**: No se manejan software propio y toda la información se maneja a través de tablas de Excel.

Efectos: Problemas para que la información se trasmita de manera rápida y confiable y las tablas de Excel con mucha información llegan a colapsar.

22. **Debilidades**: La base de datos de los Socios está alojada en un PC a través de carpetas compartidas en la red.

    Efectos: Si esta PC colapsa se pierde todo información.

23. **Debilidades:** No hay estándares definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la instalación y actualización de la configuración de las PC.

    Efectos: Al no haber estándares en cuanto a la instalación de un puesto de trabajo, puede realizarse una configuración equivocada, incurriendo en una pérdida de tiempo y productividad. Además, puede ocurrir que cada empleado del centro de cómputos instale puestos de trabajo con una configuración diferente, lo que dificultaría el mantenimiento de los mismos.

24. **Debilidades**: Para los usuarios no existen restricciones con respecto a la instalación de programas en sus respectivos puestos de trabajo, ya que están habilitados los dispositivos externos y algunos disponen de conexión a Internet sin restricciones.

    Efectos: La instalación indiscriminada de aplicaciones puede traer problemas en relación a las licencias de los programas y virus. Otro punto a tener presente es la pérdida de productividad del empleado y de recursos, ya que pueden instalarse juegos y demás programas que no hacen al funcionamiento de la empresa, arriesgando la integridad de los datos; y si el usuario posee conexión a Internet se pone en juego la confidencialidad de los mismos.

25. **Debilidades**: No hay control de acceso a la configuración del BIOS de las PC y de los servidores.

Efectos: De esta forma al momento del encendido de la máquina cualquiera podría modificar las opciones de configuración de los equipos.

26. **Debilidades**: No se realizan controles sobre los dispositivos de hardware instalados en las PC, una vez que se ha completado la instalación de algún equipo, el administrador del sistema no realiza chequeos rutinarios o periódicos.

    Efectos: Cualquier usuario podría sacar, poner o reemplazar algún dispositivo sin que se advierta la modificación.

27. **Debilidades:** No se asignan responsabilidades puntuales a cada empleado en cada tarea, ni hay un empleado del centro de cómputos designado como responsable de la seguridad de la organización.

    Efectos: Al no haber responsabilidades puntuales asignadas a cada empleado, pueden generarse malas interpretaciones con respecto a las tareas a desarrollar, lo que genera una pérdida de productividad

28. **Debilidades:** No se han desarrollado planes formales del departamento de sistemas.

    Efectos: Sin planes de sistema se genera una deficiencia en la administración de tiempo, recursos humanos, costos, etc. lo que dificulta la productividad y eficiencia del área.

29. **Debilidades**: No hay, en los empleados de la empresa, plena conciencia con respecto a la importancia de la seguridad informática.

    Efectos: Al no existir una cultura de la seguridad implementada en la empresa, no se asegura el cumplimiento de normas y procedimientos.

30. **Debilidades**: Cada vez que los usuarios necesitan asesoramiento o servicios del centro de cómputos se comunican telefónicamente con alguno de los miembros del área.

Efecto: No queda ninguna constancia de las tareas desarrolladas por los empleados del centro de cómputos, ni de las solicitudes de los usuarios.

31. **Debilidades**: En el departamento de IT no se desarrolla ningún mantenimiento preventivo.

    Efectos: Al no tener implementado un mantenimiento preventivo de los equipos y sistemas de la empresa, será necesario esperar a que ocurran los desastres para arreglarlos, lo que ocasiona pérdida de efectividad de los empleados.

32. **Debilidades:** No existe un inventario donde se documenten todos los sistemas de información y sus características principales.

    Efectos: Al generar un inventario detallado es posible discriminar los responsables de la información que administra cada sistema, las áreas en la que interviene y el nivel de prioridad con que cuenta en caso de una emergencia

33. **Debilidades:** No se han identificado las funciones más críticas para las actividades de la empresa.

    Efectos: Al no identificar las funciones que interrumpen la productividad de la empresa debido a su criticidad, se corre el riesgo de no tenerlas en cuenta en el momento de la restauración del sistema.

34. **Debilidades:** No se hacen simulaciones de siniestros.

    Efectos: Sin estas simulaciones no será posible comprobar que los empleados hayan comprendido las tareas a su cargo y será imposible predecir su comportamiento ante una emergencia.

35. **Debilidades**: En la empresa no hay planes formales para la administración de incidentes ni funciones claras que deba realizar el personal durante una contingencia, ya que no hay responsabilidades asignadas.

Efectos: Al no haberse designado claramente las responsabilidades de los empleados frente a una emergencia, las acciones que se tomen en caso de contingencia resultará caóticas, comprometiendo la integridad de los datos y equipos.

36. **Debilidades:** No se documentan los acontecimientos ocurridos durante las emergencias, ni se hacen evaluaciones formales de los daños sufridos.

    Efectos: Al no documentarse los acontecimientos ni daños acontecidos, se corre el riesgo de no hacer las correcciones necesarias para que no ocurran las mismas contingencias. Puede ocurrir también que durante el incidente se realicen modificaciones de urgencia en alguna parte del sistema y éstas no queden documentadas.

1. Análisis de Sitio Web PRODUCEPANAMA.ORG

El análisis se realizó con dos (2) aplicaciones en línea gratuitas.

- WPDOCTOR: WP Doctor es una herramienta 100% gratuita, que realiza una auditoría en tiempo real de tu WordPress y ayuda a resolver problemas de seguridad, así como mejorar la velocidad de carga, optimización del sitio y consejos sobre SEO (Optimización de Motores de Búsqueda).
- WOORANK: es una aplicación web con la que se puede generar informes de websites en los que se incluyen datos significativos sobre el estado de un sitio web así como una lista de consejos, recomendaciones a implementar con tal de optimizar la presencia online de dichos websites.

El análisis arrojó el siguiente resultado:

a) WPDOCTOR

Una Puntuación 39/100, lo que muestra grandes deficiencias en la Página web que deben ser corregidas

- **Wp- config.php protegido:** el fichero wp-config.php es accesible desde el exterior. Recomendaciones: El archivo wp-config.php, situado en la raíz de nuestro sitio desarrollado con WordPress, guarda información muy sensible de nuestra web, por lo que tendremos que procurar mantenerlo lo más seguro posible. Dentro de él se guardan información como los datos de acceso a la base de datos de WordPress (nombre de la base de datos, usuario y contraseña), claves de seguridad de WordPress y otros elementos de la configuración, como el idioma utilizado, si estamos en el modo de depuración, etc. Es necesario protegerlo, y evitar el acceso al archivo de todos los usuarios.
- **Wp-admin protegido:** El directorio /wp-admin/ es accesible sin protección. Es el que se encarga de solicitar el nombre de usuario y contraseña para identificar a los usuarios. Se usa, por ejemplo, para acceder a la administración de la web.

  Recomendaciones: Proteger el directorio wp-admin con una contraseña usando .htaccess, se puede encontrar en los servidores Apache (encriptar contraseña).

  Restringir el acceso a la administración de WordPress a determinadas IP; conectarnos a internet, a través de una determinada dirección IP, que ayuda a identificar nuestra conexión.

  Proteger el acceso de usuarios a la administración utilizando algún sistema de Captcha; añadiendo un sistema de captcha en el apartado de acceso a la administración conseguiremos evitar ataques de fuerza bruta, a menos que el robot también sea capaz de superar el captcha.

  Cambiar la página de acceso a la administración; una opción para mejorar la seguridad sería cambiar este /wp-admin por otro nombre personalizado por nosotros como /acceso.
- **Wp-login protegido:** Se puede acceder a wp-login.php sin restricciones.

Recomendaciones: Se usa, por ejemplo, para acceder a la administración de la web. Es necesario por seguridad que usuario y contraseña estén encriptadas.

- **User-agents bloqueados (WAF):** Se puede acceder usando un UA malicioso. La función de un WAF es proteger a los visitantes de la web, para que no ejecuten código malicioso, y al administrador de la web para que no puedan explotar fácilmente las vulnerabilidades de su web. Se ejecuta dentro del servidor Web. WPDoctor realiza una verificación enviando una petición al servidor con un User-Agent (nombre del software que realiza peticiones al servidor) que es habitualmente bloqueado por un WAF y así detecta si tu instalación está usando un WAF o no.

  Recomendaciones: Para evitar hackeos de Webs masivos, se recomienda un WAF, uno de los más populares es ModSecurity.

- **Information Leak:** readme. Html; license.txt; licencia.txt. Existen diversos archivos que pueden comprometer la seguridad de WordPress. Algunos archivos que se añaden con la instalación de WordPress, pero meramente informativos, y cuya información puede ser útil para los atacantes.

  Recomendaciones: Estos archivos deberíamos eliminarlos son los siguientes (license.txt; licencia.txt; readme.html). O se puede crear un directorio nuevo donde mover estos archivos o también puedes renombrarlos.

- **Cabecera Content- Security-Policy:** No tiene Cabeceras Content-Security-Policy Recomendaciones: Implementar CSP es una capa de seguridad adicional que ayuda a detectar y mitigar cierto tipo de ataques.

- **Cabecera X-Content- Type:** No tiene Cabeceras X-Content-Type: Con esta cabecera, se reduce el riesgo de que se produzca un ataque basado en confusión de tipos MIME.

- **Cabecera X-Frame:** No tiene Cabeceras X-Frame: La cabecera X-Frame-Options sirve para prevenir que la página pueda ser abierta en un frame, o iframe. De esta forma se pueden prevenir ataques de clickjacking sobre tu web.
- **Cabecera XSS:** No tiene Cabeceras X-XSS. La cabecera X-XSS-Protection se utiliza para activar el filtro XSS que tienen habilitado IE y Chrome. Se trata de una capa de seguridad adicional que bloquea ataques XSS. Internet Explorer lo implementa desde la versión 8.

  Recomendaciones: es necesario añadir cabeceras de seguridad en las líneas de código de archivos functions.php.
- **Certificado SSL:** No tiene instalado certificado o el CN no coincide con el nombre del dominio. No se detectó un certificado SSL correctamente instalado en el dominio. Es interesante tener un certificado SSL y acceder a la administración de WordPress (/wp-admin y /wp-login.php) usando HTTPS, ya que la información va encriptada y así es mucho más difícil que le roben los datos de acceso al login de WordPress.

  Recomendación: Siempre es recomendable tener instalado un certificado SSL en el web.

b) WOORANK

Ayuda a mejora la presencia en Internet, arrojando a través de un análisis puntos importantes a fortalecer.

- Plan de Marketing específicamente Seguimiento de usuarios y actividades con Google Analytics y Google Search Console. Es necesario conocer el comportamiento o cómo interaccionan los visitantes en la página. Se recomienda instalar al menos un servicio de analítica web en el sitio.
- Optimizar imágenes para la página web; asegurando que las descripciones correspondan al contenido de la imagen.

- Desarrollar estrategias de palabras clave; palabras precisas que relacionen nuestros servicios y que tengan un volumen de búsqueda aceptables.
- Mostrar las metas en la página web permiten decidir cómo describen se muestran las páginas web en los resultados de búsquedas
- Incorporar texto alternativo (atributo ALT) para que los motores de búsqueda puedan entender mejor el contenido de las imágenes.
- El tiempo carga de página es demasiado largo. Y esta es una de las principales quejas de los usuarios. Podría deberse a pobre optimización de código, problemas con el servidor, problema con red o problemas de terceros (publicidad, etc.).
- Las herramientas analíticas de Web permiten medir la actividad de los visitantes recomendamos instalar al menos una.
- No tiene seguridad SSL (HTTPS). Es recomendable para una conexión encriptada entre el navegador y los visitantes. Si la web no es HTTPS se clasificará por debajo de otras páginas.

2. Diagnóstico estado actual - ISO 27001:2013 (PRODUCE PANAMÁ)

Se realizó un diagnostico ISO (conocer el nivel de madurez) para conocer los riesgos asociados a los procesos que realiza nuestra Sociedad, este nos ayudó a:

- Conocer los activos y recursos a proteger,
- Viabilidad y eficiencia de los controles
- Conocer los niveles de riesgos aceptables
- La capacidad actual de recuperación ante incidentes
- Elaborar un plan de acción para mejorar los puntos críticos encontrados.

A continuación, presentamos el resumen de los resultados, todo en base a la condición actual de Seguridad de la Información en PRODUCE:

Se realizó un cuestionario ponderada de 0 a 5

LEYENDA	CUMPLIMIENTO
5	OPTIMIZADO
4	CORRECTO
3	INCOMPLETO
2	BORRADOR
1	PLANEADO
0	INEXISTENTE

Figura 4. Ponderación para el diagnóstico ISO 27001:2013

Arrojando como resultado la siguiente tabla.

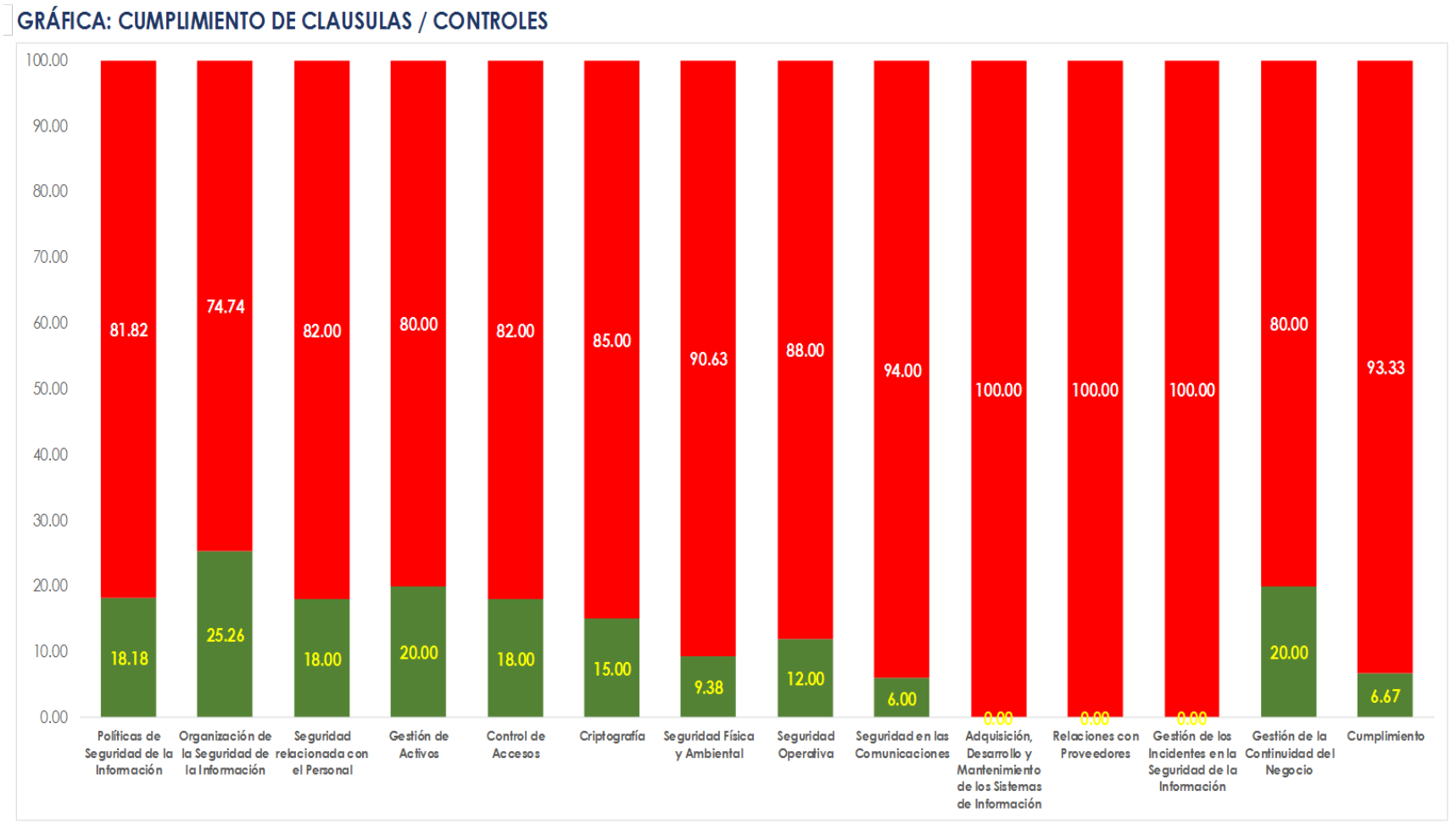
	2016
TECNOLOGÍA	0.45
Electricidad	3.00
Cableado de Datos	1.00
Networking	2.00
Centro de Datos	0.00
Servidores	0.00
Aplicaciones	0.00
Aplicaciones Web	3.00
Base de Datos	0.00
Correo Electrónico	1.00
Dispositivos de Acceso Fijos (PC)	0.72
Dispositivos de Acceso Móviles (Laptops / Celulares / Tablets / Terminales de Tarjetas)	1.00
Impresoras	1.00
Sistemas CCTV / Alarmas	0.00
Monitoreo	0.00
PROCESOS	0.92
Gestión de la Información	0.57
Service Desk	0.00
Transición	0.00
Manejo de Procesos de Seguridad Fundamentales	3.00
Certificaciones Corporativas	0.00
PERSONAL	0.44
Personal TIC	3.00
Personal en General	1.00
DOCUMENTACIÓN	1.00
Tecnología	3.00
Procesos	3.00
Personal	3.00
EVALUACIÓN FINAL	0.70 14.09%

Tabla 4. Resultados del Cuestionario

Se generó un cuadro de controles actuales aplicados en PRODUCE, presentamos los resultados

CONTROLES ISO 27001:2013			2016
Descripción	Referencia	No. Ítems	Evaluación
Políticas de Seguridad de la Información	A5	11	0.91
Organización de la Seguridad de la Información	A6	19	1.26
Seguridad relacionada con el Personal	A7	10	0.90
Gestión de Activos	A8	25	1.00
Control de Accesos	A9	20	0.90
Criptografía	A10	8	0.75
Seguridad Física y Ambiental	A11	32	0.47
Seguridad Operativa	A12	45	0.60
Seguridad en las Comunicaciones	A13	40	0.30
Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	A14	18	0.00
Relaciones con Proveedores	A15	2	0.00
Gestión de los Incidentes en la Seguridad de la Información	A16	7	0.00
Gestión de la Continuidad del Negocio	A17	6	1.00
Cumplimiento	A18	9	0.33

Tabla 5. Resultados de Controles de Seguridad



Grafica 1. Controles y Cumplimiento de Seguridad

VII. CONCLUSIÓN

Durante el desarrollo de esta Propuesta de Seguridad de la Información pudimos comprender que los recursos destinados a lograr que la información y los activos de una organización sean confidenciales, íntegros y disponibles para todos sus usuarios es un punto clave y primordial en toda organización.

Actualmente no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos, sin embargo, se debe estar preparado y dispuesto a reaccionar con rapidez ya que las amenazas y las vulnerabilidades están cambiando constantemente.

Es necesaria una política de seguridad, pero aún más importante es hacer de la seguridad, una parte importante del entorno de trabajo diario. La comunicación con los usuarios del sistema es la clave para hacer que esta política sea efectiva y se genere una "cultura de la seguridad".

Es un gran desafío implementar una política de seguridad informática en una empresa, pero es imprescindible, pues cada vez se produce un mayor número de ataques.

Todos los resultados encontrados se presentarán a la Junta Directiva de PRODUCE, y confiamos que a futuro se podrán ir implementado el plan de seguridad generado.

Nuestras expectativas personales fueron cubiertas con éxito. Fue posible aprender nuevos conceptos, desarrollando un trabajo de investigación sobre temas vigentes y volcar toda la teoría asimilada a un caso práctico.

VIII. RECOMENDACIONES

A continuación, listamos recomendaciones como parte de nuestra Propuesta de Plan de Seguridad de la Información, basándonos en los hallazgos listados y en función de las mejores prácticas internacionales:

1. Crear una red administrable, con un Servidor donde alojar los programas que se encuentran en PC de trabajo, como por ejemplo el Peachtree que está en la máquina de Contabilidad. También ayudara a disminuir costos compartiendo recursos; podemos tener un mejor control en los backups, ancho de banda. Aumentamos la seguridad y configuración de datos permitiendo a un administrador organizar los datos de la oficina más importantes. Pueden estar organizados por departamentos y evitar así que se fragmenten y acaben dispersos por todas partes. Los datos importantes pueden estar gestionados en "la parte de atrás" de un servidor y, luego, reproducirse o realizar una copia de seguridad según la política de la empresa. Igualmente, un administrador podrá controlar los datos necesarios para que puedan acceder o ser editados por empleados que tienen permiso para ello.
2. Contar con servidor que nos ayude a:
    - ✓ Centralizar la gestión de los usuarios y las contraseñas. Un servidor se encargará de gestionar todos los usuarios y sus contraseñas. Nos permitirá establecer políticas de caducidad de contraseñas, complejidad de las mismas.
    - ✓ Minimizar el número de credenciales dentro de la red: Teniendo un único servidor que se encargue de comunicarse con los distintos elementos de la red y poder usar un mismo usuario y contraseña para todo.
    - ✓ Establecer políticas en los ordenadores Windows: Desde el servidor se pueden configurar restricciones en los ordenadores de los usuarios. Por ejemplo: establecer

un mismo fondo de pantalla corporativo y que no se pueda cambiar, gestionar las actualizaciones de Windows, evitar que un usuario entre en un ordenador que no es el suyo, desactivar el acceso a pantallas de configuración de Windows.

- ✓ Centralizar los datos. Si tenemos todos los ficheros en un servidor, los usuarios podrán acceder a los mismos a través de la red sin necesidad de estar enviándose los documentos por correo electrónico. El servidor se encargará de gestionar los permisos de acceso y de registrar las conexiones. Si un ordenador de un usuario se estropease, siempre se podría acceder al servidor desde otro dispositivo y los datos no estarían comprometidos. El acceso a los datos se puede realizar tanto desde ordenadores, como de tabletas y teléfonos móviles,
- ✓ Facilidad de gestión de las copias de seguridad. Cuando tenemos todos nuestros datos en un servidor, se facilita enormemente la gestión y el mantenimiento de las copias de seguridad. Sólo hay que monitorizar un único dispositivo que contiene todos los datos críticos de la organización.
- ✓ Aplicaciones centralizadas. Si varias personas tienen que acceder, por ejemplo, al mismo programa de contabilidad, lo ideal es que este programa se instale en un servidor con todas las ventajas que hemos comentado anteriormente. No dependemos de que otro usuario tenga encendido su ordenador para poder entrar en la contabilidad.
- ✓ Gestionar el acceso remoto. Se puede configurar un servidor para permitir el acceso remoto a los datos mediante conexiones seguras por VPN. De esta manera, un usuario con los permisos adecuados, podría conectarse al servidor desde el ordenador de su casa para terminar una oferta que había dejado pendiente.

3. Sería conveniente que las entradas de USB y lectoras de discos se deshabilitaran desde el BIOS de cada máquina. Si llega a ser necesario, para realizar alguna tarea de mantenimiento, el administrador de sistemas puede ingresar al BIOS del equipo (utilizando la contraseña que él suministró), habilitar el dispositivo necesario y, una vez utilizado, deshabilitarlo nuevamente.
4. Una red mixta es la mejor opción. No se deben pensar en los dos tipos de red como excluyentes, sino complementarios. La red empresarial debería empezar con un sistema de cableado estructurado, al que se conectarán generalmente los servidores de aplicaciones y la mayoría de los computadores de escritorio. Complementaremos luego esta red con uno o varios puntos de acceso WiFi, que se utilicen para permitir la conexión de los equipos móviles, como portátiles, netbooks, PDAs y teléfonos móviles.
5. Las tareas de mantenimiento de las PC de los puestos de trabajo deberían ser llevadas a cabo por el administrador del centro de cómputos, o por alguien designado por él.
6. Sugerimos que se documente cada uno de estos cambios, para así tener un control y una identificación de los mismos, así se podrá generar un historial de modificaciones.
7. Consideramos necesario que exista un procedimiento escrito y formal de política de backup, que contenga las recomendaciones que se describen a continuación:
    - ✓ Sería conveniente que el Jefe del departamento de Informática designe a un responsable de la realización de las copias de seguridad y de su restauración, y un suplente de éste primero.
    - ✓ El procedimiento de generación de backup debería estar automatizado con alguna herramienta de generación de copias de respaldo de datos.

- ✓ Debería realizarse un backup incremental diario, todos los días de la semana, mientras que una vez por semana sería conveniente realizar un backup completo de los datos más significativos.
- ✓ Deberían realizarse chequeos para comprobar que los procedimientos de restauración son eficientes.
- ✓ Los archivos de backup deberían tener una contraseña que los proteja, o bien encriptarse, ya que contienen información confidencial.
- ✓ Los backups diarios deberían almacenarse en el exterior de la empresa, ya que poseen un empleado designado, sería conveniente contar con un suplente.
- ✓ Sugerimos que este empleado se lleve el último backup realizado, mientras que los demás CD deberían permanecer en el interior de la empresa resguardados en un lugar ajeno al centro de cómputos. Consideramos necesario que el CD que es llevado al exterior sea transportado en un medio resistente que lo proteja.
- ✓ Deberían realizarse chequeos para comprobar el funcionamiento correcto de los medios externos donde se realizan las copias de respaldo.
- ✓ Debería existir una política de reemplazo de CD, donde conste que deberían reemplazarse cada 6 meses, para evitar posibles fallas en el momento de la recuperación, debido al tiempo de vida útil del medio.
- ✓ Debería existir un procedimiento de recuperación de copias de respaldo, donde se incluya la metodología a seguir, quién tiene el permiso para realizarlo y en qué casos será permitido.
- ✓ Debería existir documentación de los backups generados, incluyendo:
    - Qué datos contienen estas copias

- Fechas de realización,
- Fechas de restauración,
- Errores obtenidos,
- Tiempo empleado en el proceso,
- Demás datos que se consideren necesarios en la administración de este procedimiento.

8. Generar un plan de monitorización, teniendo en cuenta que la monitorización tiene un impacto directo en la performance del sistema. Se podría utilizar, por ejemplo, alguna herramienta para monitorizar el tráfico y rendimiento de red, como un escáner de seguridad integral (Overall Security Scanner).
9. Sugerimos que la documentación posea más detalles respecto a los siguientes datos:
    - ✓ Diagrama de la distribución física de las instalaciones, identificación de PC y equipos, y puestos de trabajo
    - ✓ Número de serie de hardware
    - ✓ Número de licencia del software
    - ✓ Inventario de "hardware" y "software"
    - ✓ Fallas en equipos y trabajos de mantenimiento
    - ✓ Entrada del personal externo
    - ✓ Configuración de equipos y servidores
    - ✓ Cambios en la topología de red
    - ✓ Modificaciones de emergencia realizadas a sistemas y hardware
    - ✓ Métodos para compartir datos entre sistemas (entre las sucursales o entre las PC´s de la red)

10. Sugerimos que la documentación posea más detalles respecto a los siguientes datos:
    - ✓ Plan de contingencia
    - ✓ Política de seguridad
    - ✓ Manual de procedimientos
    - ✓ Manual de usuario (del software y del hardware)
    - ✓ Manual de seguridad para el sistema: detalla las funciones y privilegios de la seguridad. Contiene: configuración, administración y operación del sistema, guías para el buen uso de las características de protección del sistema, etc.
    - ✓ Manual de seguridad para el usuario: asiste a los usuarios del sistema, describe cómo usar las protecciones, las responsabilidades de la seguridad del sistema.
11. El Samba podría utilizarse para el control de perfiles. Con esta aplicación podría gestionarse la protección de las distintas carpetas, incluyendo las de backup de la página Web y de los usuarios, con controle de acceso más fuertes que los que están funcionando en la futura red; esto se logra declarando la aplicación como controladora de dominios, para que administre las carpetas, con una funcionalidad similar a la de Linux.
12. Puede ser útil que el SendMail asocie una cuenta de mail a una PC determinada, de manera que solo pueda usarse ese equipo en particular para leer o enviar mails desde esa cuenta.
13. Debería controlarse que el servicio de mails se use solo para fines laborales, notificando a los usuarios de esta norma. Además, sería conveniente hacerle advertencias con respecto a la suscripción a listas de correo. Se podría calcular una estadística del nivel medio de tráfico de red generado por el correo electrónico, de manera que aquel usuario que sobrepase la media será evaluado para controlar si el uso que le da a este servicio es el correcto. De no ser así deberían tomarse las acciones correctivas respectivas.

14. El SendMail podría configurarse para que aquellos mensajes enviados por la gerencia o los que tienen ciertos destinatarios, como fábricas o bancos, se envíen con prioridad alta.
15. Podrían realizarse backups solo los mensajes con prioridad alta que se almacenan en el servidor de Internet.
16. Podría utilizarse firma digital o encriptación para los mensajes con prioridad alta de las cuentas de correo de la Gerencia, y así poder realizar un envío seguro al transmitir documentos confidenciales. Por ejemplo, podrían comprimirse la información de los mensajes para que no viaje en texto plano y protegerla con una contraseña para mayor seguridad.
17. La actualización de las listas de virus debería ser responsabilidad del administrador o de un empleado del área de sistemas designado por él. Éste debería, además, realizar chequeos aleatorios verificando que las listas de virus estén actualizadas y que se realicen periódicamente escaneos en busca de virus. Estas tareas deben realizarse tanto en las PC como en los servidores.
18. Debería haber un procedimiento documentado a seguir para el caso que se encuentre un virus en el sistema. Sugerimos las siguientes actividades:
    - ✓ Chequear el disco con el escaneo de virus para determinar si hay un virus, y qué virus es. Eliminar el virus.
    - ✓ Cerrar los programas, apagar la máquina y bootear la computadora desde el disco de rescate del antivirus.
    - ✓ Hacer un nuevo chequeo de virus en el disco duro.
    - ✓ Chequear el resto de los dispositivos de datos (disqueteras, discos removibles, etc.), para saber de dónde vino el virus.

- ✓ Tratar de determinar la fuente del virus. La persona que hizo llegar el virus debe ser informada.
- ✓ Avisar a todos los usuarios del sistema que hayan intercambiado datos con la computadora infectada.
- ✓ Si el virus borró o modificó algún dato, tratar de restaurarlo desde los backups y restaurar los programas involucrados.
- ✓ Hacer un nuevo escaneo del disco, buscando virus en los datos restaurados.

19. Sería recomendable implementar un régimen de separación de tareas, para que un usuario no pueda realizar el ciclo de vida completo de una operación, y necesite de la intervención de otros empleados para poder concretarla, de manera que para poder realizar un fraude es necesaria la participación de más de un empleado, y se agrega un control para evitar posibles errores. Para esto será necesario restringir permisos a los usuarios. Sería bueno tener en cuenta otro control, como la rotación de personal para controlar el desempeño que los empleados han tenido durante un período de tiempo. Además, sirve para tener una persona capacitada de respaldo, en caso de necesitar una suplencia. Para poder llevar a cabo este control es necesario cambiar el usuario de grupo, modificándole sus permisos. Estas tareas deberían estar a cargo del Departamento de Recursos Humanos, junto con los directivos de la empresa o con los responsables de cada área.
20. El archivo de datos de empleados y socios debería estar encriptado, y la carpeta donde se almacena debería tener una clave de acceso.
21. Invertir en Software para la empresa e instalarlo en el Servidor creando políticas de acceso por departamentos.
22. Invertir en un Sistema de base de datos creando políticas de acceso por departamento

23. Sugerimos desarrollar un procedimiento formal a seguir cada vez que sea necesario instalar un nuevo puesto de trabajo en la empresa, o reparar alguna PC con errores de configuración, con el fin de establecer un estándar. Podría utilizarse, como complemento, alguna herramienta de restablecimiento y copia de configuración Sería recomendable documentar, no solo el procedimiento de instalación y reparación de puestos de trabajo, sino además cada uno de los mantenimientos que se les realizan, a modo de historial de cada PC. Con esto se logra una documentación de la configuración actual de cada una de las máquinas.
24. Para evitar la instalación de programas no deseados, es recomendable que, en el momento que el usuario ingresa a la empresa, se lo notifique y acepte que está prohibida la instalación de cualquier producto de software en los equipos. Con este requerimiento es posible tomar medidas a posteriori de la infracción, además de ayudar a generar una "cultura de la seguridad". Sugerimos que algún encargado del centro de cómputos designado por el administrador, realice chequeos periódicos de las PC´s, identificando así los nuevos productos que han sido instalados. Además, sería conveniente instalar una herramienta que audite en forma automática y constante las PC´s en busca de modificaciones y genere reportes cada vez que suponga un problema, de esta manera no se necesitará realizar los chequeos con tanta frecuencia
25. Sería conveniente que las máquinas tuvieran configurado un password de administrador en el acceso al setup (BIOS), para evitar que se modifiquen las configuraciones base de los equipos, esto podría aplicarse tanto a las PC´s como a los servidores. Estas contraseñas deberían gestionarlas el administrador del sistema, en todos los equipos de la red.

26. Sería conveniente que el administrador, o algún encargado de cómputos designado por él, realice chequeos periódicos para comprobar la correcta instalación de los dispositivos de los equipos, su buen funcionamiento y que sus números de series se correspondan con los datos registrados por el administrador al momento de la instalación.
27. Deberían designarse responsabilidades claras y documentadas para cada empleado del centro de cómputos, las que deberán constar en los procedimientos formales que se desarrollen para cada actividad. De acuerdo a las funciones que desempeñen deberán distribuirse los permisos particulares de cada uno de los usuarios en sus respectivas cuentas del sistema. Además, debería haber un empleado a cargo de la seguridad del sistema, que coordine las tareas relativas a este tema, haciendo cumplir las políticas de seguridad en toda la empresa.
28. Una medida de control útil sería desarrollar un plan de sistemas a corto plazo, que permita una supervisión continua y directa de las tareas que realiza el personal del centro de cómputos, y que contenga un cronograma de las actividades del área, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante un periodo no muy prolongado de un año, debido a las cambiantes exigencias del sector. Además, podría considerarse el desarrollo de un plan estratégico a largo plazo, que contenga los proyectos principales y los cronogramas de su implementación, para un periodo de por lo menos 3 años.
29. A pesar de que existe una cierta conciencia sobre la seguridad de la información en el sector gerencial de la empresa, el equipo de sistemas debe hacer hincapié en la concienciación de todos los usuarios, haciéndolos más responsables y partícipes de las medidas de seguridad, ya que son los principales involucrados, tanto los usuarios actuales como los que se

incorporen en el futuro. El proceso de concienciación debería ser renovado y transmitido a los usuarios en forma anual para asegurar que todos los usuarios que están afectados tengan acceso a las novedades sobre aspectos de seguridad

30. Sería conveniente que los usuarios envíen mails al centro de cómputos, solicitando asesoramiento o servicios, o para reportar incidentes o problemas con sus equipos, de manera que quede constancia de la misma. Además, debería llevarse un registro de los trabajos efectuados por los empleados del centro de cómputos, es decir tener algún tipo de mecanismo o historial de reportes. Podría ser útil y eficiente la implementación de un buzón de sugerencias (por ejemplo, una dirección de correo), donde los usuarios puedan recomendar mejoras o realizar cualquier tipo de comentarios, expresando sus inquietudes.
31. Cuando finalice el desarrollo, alguno de los empleados podría asumir la responsabilidad de llevar a cabo un mantenimiento preventivo, monitorizando, chequeando y auditando las PC´s y demás dispositivos que conforman la red
32. Es conveniente la generación de un inventario donde se detallen los sistemas de información utilizados en la organización, documentando las siguientes características:
    - ✓ Nombre
    - ✓ Lenguaje
    - ✓ Departamento de la empresa que genera la información (dueño del sistema)
    - ✓ Departamentos de la empresa que usan la información
    - ✓ Volumen de archivos con los que trabaja
    - ✓ Volumen de transacciones diarias, semanales y mensuales que maneja el sistema
    - ✓ Equipamiento necesario para un manejo óptimo del sistema
    - ✓ La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.

- ✓ El nivel de importancia estratégica que tiene la información de este sistema para la Institución (medido en horas o días en que la institución puede funcionar adecuadamente, sin disponer de la información del sistema)
- ✓ Relación de equipamiento mínimo necesario para que el sistema pueda seguir funcionando. Será necesario mantener esta relación siempre actualizada
- ✓ Actividades a realizar para volver a contar con el sistema de información (actividades de restauración)
- ✓ Puede ser útil disponer de un responsable a cargo de la actualización del mismo, que controle periódicamente estos dispositivos y la información almacenada

33. Definir las funciones o servicios de la empresa que sean más críticos. Cada jefe o encargado de área debe interactuar con el administrador y definir estos servicios junto con los recursos mínimos necesarios para su funcionamiento, y asignarles una prioridad en el plan de restauración. Además, sería conveniente identificar las contingencias que podrían ocurrir para cada nivel de servicio determinando, considerando:
    - ✓ Cuáles serían los peores problemas a los que se puede ver sometida la empresa, cuáles serían las peores contingencias
    - ✓ Cuáles serían las más probables
    - ✓ Cuáles son las que ocurren más a menudo
    - ✓ Cuáles son las que no ocurren nunca
34. Para el entrenamiento del personal deberían generarse simulacros de siniestros y así evaluar la efectividad del plan.
35. Debería conformarse un plan de emergencias, determinando los procedimientos a llevar a cabo para cada contingencia identificada en la estrategia proactiva. Estas tareas deberían

estar claramente definidas y documentadas, y tener asignado un responsable para su ejecución, considerando los distintos escenarios posibles (por ejemplo durante el día o la noche). Ejemplos de las tareas a desarrollar pueden ser:

- ✓ En caso de incendio:
  - Identificar las vías de salida
  - Generar un plan de evacuación del personal
  - Desarrollar un plan de puesta a buen recaudo de los activos
  - Ubicación y señalización de los elementos contra el siniestro
- ✓ En caso de intrusión interna o externa:
  - Desconectar los servidores
  - Cerrar todos los accesos a los datos
  - Rastrear al intruso
- ✓ Deberían contemplarse las siguientes características:
- ✓ Debería estar documentado y testeado antes de su puesta en práctica.
- ✓ Debería basarse en un análisis de riesgo, determinando que acciones merecen estar incluidas.
- ✓ Debería abarcar toda la empresa, no solo el área de cómputos.
- ✓ Debería entrenarse a los responsables y a los usuarios
- ✓ Debería mantenerse actualizado de acuerdo a nuevos puestos de trabajos y funciones.
- ✓ Debería ser retroalimentarlo después de cada incidente.
- ✓ Debería ser probado frecuentemente.
- ✓ Debería contener la siguiente información:

- Objetivo del plan.
- Modo de ejecución.
- Tiempo de duración.
- Costes estimados.
- Recursos necesarios.
- Evento a partir del cual se pondrá en marcha el plan.

36. Sugerimos que se documente la realización de las siguientes actividades después de que ha ocurrido algún desastre:

    ✓ Determinar la causa del daño.

    ✓ Evaluar la magnitud del daño que se ha producido.

    ✓ Que sistemas se han afectado.

    ✓ Qué modificaciones de emergencia se han realizado.

    ✓ Que equipos han quedado no operativos,

    ✓ Cuales se pueden recuperar y en cuanto tiempo.

    Se debería actualizar la documentación del Departamento de IT con las modificaciones implementadas y las acciones correctivas que se llevaron a cabo como consecuencia del incidente.

A. Diseño del Plan de Seguridad

En esta Propuesta de Plan de Seguridad de la Información se desarrollan normas y procedimientos que pautan las actividades relacionadas con la seguridad informática y la tecnología de Información. Este deberá ser aprobado por los directivos de La Sociedad Panameña de Productores Fonográficos para su implementación y futura ejecución.

Estas políticas de seguridad informática y las medidas de seguridad en ellas especificadas deben ser revisadas periódicamente, analizando la necesidad de cambios o adaptaciones para cubrir los riesgos existentes y auditando su cumplimiento.

1. Medidas necesarias a implementar a Corto Plazo.

a) Networking

- Deberá existir documentación detallada sobre los diagramas topológicos de la red.
- La conectividad a Internet será otorgada para propósitos relacionados con el negocio y mediante una autorización de la Gerencia. Los usuarios no autorizados deberán estar imposibilitados de conectarse al exterior.
- Los usuarios de la organización que utilicen Internet deben recibir capacitación específica respecto a su funcionalidad y a los riesgos y medidas de seguridad pertinentes.
- Deben documentarse los servicios provistos a través de Internet y definirse las responsabilidades en cuanto a su administración.
- Cada vez que se establezca una vía de comunicación con terceros (personal de mantenimiento externo, fábricas, proveedor de servicios de Internet, etc.), los mecanismos de transmisión y las responsabilidades de las partes deberán fijarse por escrito.
- La información enviada a través de equipos de comunicaciones de la empresa se considera privada. Cabe aclarar que la información no es pública, a menos que en forma expresa se indique lo contrario.
- Se debe instalar un Firewall para brindar un nivel adicional de seguridad a la red de la Sociedad. A través del mismo, se puede activar Web Filtering para restringir la navegación en Internet.

- El uso de Internet debe ser monitoreado periódicamente. Si existe alguna razón para creer que la seguridad está siendo violada, la compañía puede revisar el contenido de las comunicaciones de Internet.
- El acceso casual a los mensajes de correo electrónico por los administradores y similares, se considera una violación a la política de seguridad de la información. Sin embargo, la Gerencia tiene el derecho de examinar cualquier información, sin previo consentimiento o notificación del empleado, en caso que se considere que se está utilizando inadecuadamente el equipamiento de la compañía.
- Deben tomarse los recaudos necesarios para restringir todo tipo de aplicaciones que no ayudan al cumplimiento de los objetivos de la organización, tales como herramientas de chateo o "file sharing".

b) Servidores

- Para mejorar el trabajo y la organización, al tener centralizados los datos y recursos se recomienda invertir en servidores de datos.
- No deben existir usuarios "administradores" con ese nombre, con el fin de despistar a los atacantes.
- Se deben bloquear todos los servicios/puertos innecesarios, y asegurar que sólo personas autorizadas tengan acceso a información sensitiva.

c) Aplicaciones

- Se deben seguir las recomendaciones de seguridad para la página web de la Sociedad, con el fin de resguardar los datos expuestos y la reputación online de la Sociedad.
- Deberá existir un procedimiento formal para dar de alta y de baja las cuentas de correo electrónico en el sistema informático.

- El administrador de mail no debe ser utilizado para enviar correo basura (SPAM).
- Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
- El correo electrónico no debe ser utilizado para enviar cadenas de mensajes no debe relacionarse con actividades ilegales y no éticas o para mensajes no relacionados con los propósitos de la empresa.
- Los datos que se consideraron “confidenciales” o “críticos” deben encriptarse.
- Las computadoras portátiles deben mantener el disco cifrado. Cualquier disco duro externo o USB que se utilice en la Sociedad debe seguir el mismo lineamiento de cifrado.
- En todos los equipos de la empresa debe existir una herramienta antivirus ejecutándose permanentemente y en continua actualización.
- La actualización de los antivirus de todos los equipos de la empresa deberá realizarse a través de un procedimiento formal y, si es posible, automático, a cargo de un empleado del centro de cómputos designado por el administrador.
- Deberán programarse escaneos periódicos de virus en todos los equipos de la empresa; esta tarea estará a cargo de personal designado por el administrador del centro de cómputos.
- Deberá existir un procedimiento formal a seguir en caso que se detecte un virus en algún equipo del sistema.
- Deberá existir una clasificación de los datos en base a su sensibilidad para definirlos como críticos y así determinar controles específicos. Se deberán definir tres niveles de información:
    - ✓ Crítica:

- la no-disponibilidad de esta información ocasiona un daño en los activos de la empresa;
- se considera recurso crítico a aquel recurso interno que debe estar disponible solamente para un conjunto determinado de personas, debe ponerse un cuidado especial en información que por ley o que por políticas de la empresa debe permanecer confidencial; la clasificación de un recurso como crítico deberá incluir los criterios para determinar quiénes tienen acceso a él. De ser necesaria su transmisión por redes externas o su almacenamiento en sistemas de la red perímetro, deberán tomarse medidas de seguridad extremas, la información deberá encriptarse;

✓ Confidencial:

- en poder de personas no autorizadas compromete los intereses de la empresa;
- Se considera recurso confidencial a todo aquel que solo deberá utilizarse y ser del conocimiento de miembros de la empresa y por defecto todo aquel recurso que no haya sido explícitamente clasificado como disponible al público;

✓ Pública:

- información de libre circulación;
- se considera recurso disponible al público aquel que no requiere permanecer como de uso interno y que explícitamente se ha clasificado como un recurso público.

Esta clasificación deberá ser documentada e informada a todo el personal de la organización, y deberá evaluarse y actualizarse periódicamente.

- Deberá existir un responsable en cada área de la empresa, que responda por la información que se maneja en dicho sector. Deberá definir la clasificación de los datos y los controles de acceso que son necesarios, junto con el administrador del sistema.
- Deberán existir estándares de configuración de los puestos de trabajo y demás equipos de la red informática.
- En base al estándar se deberá generar un procedimiento donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.
- Las aplicaciones solo se actualizarán debido al reporte de algún mal funcionamiento o a un nuevo requerimiento por parte de los usuarios o del personal del centro de cómputos.
- Se deberán documentar no solo el procedimiento de instalación y reparación de equipos, sino además cada uno de los mantenimientos que se les realicen. Deberán generarse historiales y así calcular datos estadísticos de los cambios realizados y los errores reportados.
- En el momento en que un nuevo usuario ingrese a la empresa, se lo debe notificar y deberá aceptar que tiene prohibida la instalación de cualquier producto de software en los equipos.
- Se deberán realizar chequeos periódicos en las PC´s, y demás equipos, en búsqueda de aplicaciones instaladas no autorizadas o innecesarias.
- Se deberá asegurar la existencia de un procedimiento aprobado para la generación de copias de resguardo sobre toda la información necesaria para las operaciones de la organización,

donde se especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas.

- La periodicidad de la generación de los resguardos debe ser acorde a la criticidad de la información y la frecuencia de cambios.
- La ubicación de los backups debe contar con adecuadas medidas de seguridad, sin estar expuestos a las mismas contingencias que el centro de cómputos, es decir que deberán almacenarse en el exterior de la empresa, y ser transportados en un medio resistente que los proteja. Debe designarse un responsable y un suplente encargados de su custodia, y se generará un registro de los movimientos de estos medios.
- Los archivos de backup deben tener un control de acceso lógico de acuerdo a la sensibilidad de sus datos, además de contar con protección física.
- El administrador del centro de cómputos debe designar un responsable de la realización de las copias de seguridad y de su restauración, y un suplente de éste primero.

d) Personal Administrativo

- Debe existir una adecuada y documentada separación de funciones dentro del centro de cómputos.
- El área de sistemas debe encontrarse ubicada en el organigrama de la empresa en una posición tal que garantice la independencia necesaria respecto de las áreas usuarias.
- Deberá realizarse una rotación en las tareas del personal del centro de cómputos para controlar el desempeño que los empleados han tenido durante un período de tiempo. Para esto se deberán establecer períodos de vacaciones anuales obligatorios para el personal del área, entre otras medidas.

- La Gerencia determinará que empleados deben contar con una cuenta de correo electrónico, según lo amerite su tarea.
- Deberá existir un procedimiento formal para dar de alta y de baja las cuentas de correo electrónico en el sistema informático.
- Deberá existir una adecuada protección física y mantenimiento permanente de los equipos e instalaciones que conforman los activos de la empresa.
- Se deberá restringir el acceso físico a las áreas críticas a toda persona no autorizada, para reducir el riesgo de accidentes y actividades fraudulentas.
- Las disqueteras y lectoras de CD deberán deshabilitarse en aquellas máquinas en que no se necesiten.
- Las PC´s de la empresa deberán tener un password de administrador en el BIOS, que deberá gestionar el administrador del sistema.
- Los usuarios finales no deben contar con usuarios administrador, sólo el personal de Tecnología.
- El personal del centro de cómputos debe mantenerse capacitado respecto de las tecnologías utilizadas en la organización.
- Debe impartirse capacitación a los usuarios finales a efectos de que puedan operar adecuadamente los recursos informáticos.
- El personal debe ser entrenado respecto al cumplimiento de lo especificado en la política de seguridad informática. Se debe entregar una copia de la misma a cada empleado.
- Se debe obtener un compromiso firmado por parte del personal respecto al cumplimiento de las medidas de seguridad definidas en la política de seguridad informática, destacando específicamente el mantenimiento de la confidencialidad de las claves de acceso, la no-

divulgación de información de la organización, el cuidado de los recursos, la utilización de software sin licencia y el reporte de situaciones anormales. Debe confirmarse este compromiso anualmente o cada vez que se produzcan cambios en las funciones asignadas al personal.

- Asegurar que los empleados reciban capacitación continua para desarrollar y mantener sus conocimientos competencia, habilidades y concienciación en materia de seguridad informática dentro del nivel requerido a fin de lograr un desempeño eficaz.

e) Documentación

- Deberá utilizarse un plan detallado de sistemas, donde se definan las asignaciones de recursos, el establecimiento de prioridades y responsabilidades, la administración de tiempos y la utilización de métricas de software. Esta norma deberá aplicase tanto para el desarrollo de las aplicaciones como para las modificaciones que se realicen.
- Deberá existir un documento formal de solicitud de cambios, donde quede reflejado el motivo y la solicitud del cambio, allí se agregarán los requerimientos de seguridad necesarios, definidos por el responsable de la información y el administrador de sistemas. La documentación de los cambios debe incluir:
    - ✓ sistema que afecta,
    - ✓ fecha de la modificación,
    - ✓ desarrollador que realizó el cambio,
    - ✓ empleado que solicitó el cambio,
    - ✓ descripción global de la modificación.

- Se deberá informar por escrito la importancia de la seguridad de la información a todo el personal contratado, terceros y consultores. El administrador del centro de cómputos, junto con los directivos, serán quienes:
    - ✓ especifiquen los requerimientos de seguridad,
    - ✓ determinen los pasos a seguir en caso que no se respete lo establecido en el contrato,
    - ✓ establezcan cláusulas sobre confidencialidad de la información,
    - ✓ exijan al tercero en cuestión que informe posibles brechas de seguridad existentes.
- Los contratos con terceros deberán contener una cláusula que indique "Derecho de auditar el desempeño del contratado".
- Con respecto a la contratación de terceros para el desarrollo de aplicaciones, éste deberá entregar a la empresa:
    - ✓ aplicación ejecutable,
    - ✓ código fuente de la aplicación,
    - ✓ documentación del desarrollo,
    - ✓ manuales de uso.
- Antes de realizar la compra de una aplicación de software, deberá:
    - ✓ realizarse un análisis de costo – beneficio,
    - ✓ comprobar la adaptabilidad a los sistemas existentes en la empresa,
    - ✓ verificar la compatibilidad con los sistemas operativos de la empresa,
    - ✓ evaluar las medidas de seguridad que posee,
    - ✓ asegurar un servicio post-venta apropiado,
    - ✓ solicitar la misma documentación que se exige a los terceros.
- Deberá existir un procedimiento manual de respaldo para realizar las tareas cotidianas.

- Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en el centro de cómputos.
- Deberán existir una documentación y un registro de las actividades del centro de cómputos (procesos normales, eventuales y excepcionales) que se desarrollan diariamente, que incluya como mínimo el detalle de los procesos realizados.
- Deberá desarrollarse documentación detallada sobre el equipamiento informático, que consista en diagramas y distribución física de las instalaciones, inventarios de hardware y software, diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos. Esta documentación comprende tanto al centro de procesamiento de datos principal, como a los secundarios y las redes departamentales.
- Deberá existir un registro de los eventos, errores y problemas del hardware y el software utilizados en las operaciones de procesamiento de datos.
- La metodología para el desarrollo y mantenimiento de sistemas debe incluir estándares para la documentación de las aplicaciones y las actividades. Esta documentación deberá mantenerse actualizada y abarcar todas las fases del ciclo de vida del desarrollo de los sistemas.

2. Medidas necesarias a implementar a Largo Plazo

a) Networking

- Se deberá asegurar la integridad, exactitud, disponibilidad y confidencialidad de los datos transmitidos, ya sea a través de los dispositivos de hardware, de los protocolos de transmisión, o de los controles aplicativos.

- Una red mixta es la mejor solución (cables y wifi) los dos tipos de red no son excluyentes como excluyentes, sino complementarios. La red empresarial deberá empezar con un sistema de cableado estructurado, al que se conectarán generalmente los servidores de aplicaciones y la mayoría de los computadores de escritorio. Se complementará luego esta red con uno o varios puntos de acceso Wi-Fi, que se utilicen para permitir la conexión de los equipos móviles, como portátiles, netbooks, PDAs y teléfonos móviles.
- Las redes Wifi se deben utilizar en las siguientes situaciones:
    - ✓ Con empleados que usan PC portátil u otro dispositivo móvil, y necesitan desplazarse con él a diversos puntos de la oficina.
    - ✓ Si hay ejecutivos con puestos fijos, que principalmente necesitan acceso a Internet en sus portátiles, pero muy rara vez requieren compartir archivos grandes con otros usuarios o descargarlos desde un servidor interno.
    - ✓ En la sala de juntas, donde habitualmente se reúnen visitantes y empleados de la compañía para hacer presentaciones, compartir datos, intercambiar archivos, etc.
    - ✓ Utilizar enlaces inalámbricos cuando la movilidad sea imprescindible. Para todos los demás casos, una conexión por cable le dará mejores resultados.
- Deberán existir medios alternativos de transmisión en caso de que alguna contingencia afecte al medio primario de comunicación.
- Debe asegurarse que la totalidad del tráfico entrante y saliente de la red interna, sea filtrado y controlado por un firewall prohibiendo el pasaje de todo el tráfico que no se encuentre expresamente autorizado.
- Todas las conexiones a Internet de la empresa deben traspasar un servidor Proxy una vez que han traspasado el firewall.

- No se publicarán en Internet datos referidos a las cuentas de correo de los empleados.
- De ser necesario realizar mantenimiento remoto a los futuros servidores, se utilizarán protocolos y servicios de comunicación que garanticen la seguridad de los datos que se transmiten a través de la red, utilizando encriptación. Deberán documentarse cada una de las actividades que el personal externo realice sobre los equipos utilizando acceso remoto. Para llevar a cabo estas tareas, el encargado del mantenimiento deberá solicitar formalmente la dirección IP del servidor de Internet y el password de la cuenta de mantenimiento al administrador del centro de cómputos.
- El esquema de direcciones de la red interna no debe ser visible ante las conexiones externas.
- Deberá asegurarse que la dirección IP de la empresa sea un número variable y confidencial.
- Los recursos lógicos o físicos de los distintos puestos de trabajo no deben ser visibles en el resto de la red informática. Los recursos de los servidores serán visibles solo en los casos necesarios y con las medidas de seguridad correspondientes.
- El cableado debe seguir las normas del cableado estructurado, que garantizan el funcionamiento eficiente de la red.
- Si el tendido del cableado se terceriza, la empresa encargada debe prestar garantías escritas sobre su trabajo.
- Se deberá documentar en planos los canales de tendidos de cables y las bocas de red existentes.
- Debe existir tendido de cableado redundante para futuros puestos de trabajo. Estos cables no deben tener bocas de red instaladas.
- Deberá medirse periódicamente el nivel de interferencia que existe en la red. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.

- Deberá medirse periódicamente nivel de ancho de banda de red ocupado. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.
- En el caso de ocurrir esta contingencia con la continuidad del servicio de red, deberá existir un sistema informático off line para los sectores críticos de la empresa.

b) Servidores

- Se necesita crear perfiles de usuario (administrador, gerencia, empleados) y establecer políticas de uso para datos, dispositivos conectados a la red, etc. Es decir, que los usuarios puedan acceder a según su tipo de usuario a la información que necesiten para su actividad.
- Ya que algunos empleados comparten documentos en diferentes ordenadores, se podrá evitar que algún día por error, un documento se borre o que existan varias versiones del mismo documento. Necesitas un servidor que centralice la creación y modificación de documentos.
- Ayudará a crear copias de seguridad de los datos y posibilidad de restauración y recuperación ante desastres. Programar las copias por días, frecuencia semanal o mensual dependiendo de los departamentos. Lo ideal es que los datos se almacenan en el local en el hardware encargado de realizar las copias de seguridad y al mismo tiempo, se duplica la información en un centro de datos remoto.
- Los servidores deberán tener una llave de bloqueo de hardware.
- Los gabinetes donde se ubican los switches de cada una de las sucursales, deberán permanecer guardados bajo llave, y fuera del alcance de personal no autorizado
- El administrador o algún encargado de cómputos designado por él, deberá realizar chequeos periódicos para comprobar:
    - ✓ la correcta instalación de los dispositivos de los equipos,

- ✓ su buen funcionamiento,
- ✓ sus números de series corresponden con los datos registrados por el administrador al momento de la instalación.

- Los servidores deberán apagarse automáticamente una vez que han cerrado toda la oficina.
- Es necesario adecuar el salón o cuarto donde estará el o los servidores,

  Deberán existir los siguientes dispositivos de soporte en la empresa:

  - ✓ Aire acondicionado: en el centro de cómputos la temperatura debe mantenerse entre 19º C y 20º C.
  - ✓ Matafuegos: deberán ser dispositivos químicos y manuales que cumplan las especificaciones para extinguir incendios en equipos eléctricos de computación,
    - deberán estar instalados en lugares estratégicos de la empresa,
    - el centro de cómputos deberá contar con uno propio ubicado en la habitación de los servidores.
  - ✓ Alarmas contra intrusos: deberán contar con una alarma que se active en horarios no comerciales. Ésta deberá poder activarse manualmente en horarios laborales ante una emergencia.
  - ✓ Generador de energía: deberá existir un generador de energía que se pondrá en marcha cada vez que haya problemas con el suministro de energía eléctrica o avisos de cortes de luz.
  - ✓ UPS: (Uninterruptible power supply) deberá existir al menos un UPS en el centro de cómputos que atienda a los servidores, con tiempo suficiente para que se apaguen de forma segura.

- ✓ Luz de emergencia: deberá existir una luz de emergencia que se active automáticamente ante una contingencia.
- ✓ Estabilizador de tensión: deberá existir al menos un estabilizador de tensión que atienda la línea de energía eléctrica independiente del centro de cómputos.
- ✓ Descarga a tierra: deberán existir métodos de descarga a tierra para el edificio y otra independiente para el centro de cómputos.

- Todos estos dispositivos deberán ser evaluados periódicamente por personal de mantenimiento.
- Deberá existir una llave de corte de energía general en la salida de emergencias del edificio.
- No deberán utilizarse los servidores de la empresa como medios de almacenamiento de las copias de respaldo de ningún sistema.

c) Aplicaciones

- La empresa deberá contar con un sistema de mail externo y uno interno, con diferentes dominios. De esta manera, las comunicaciones entre el personal de la empresa se realizarán sin exponer los mensajes a Internet.
- Los aplicativos de correo electrónico deben brindar las condiciones de seguridad necesarias para evitar los virus informáticos o la ejecución de código malicioso, deben brindar la facilidad de impedir que un usuario reciba correos de un remitente riesgoso para los recursos de la empresa.
- Todas las cuentas de correo que pertenezcan a la empresa deben estar gestionadas por una misma aplicación. Esta debe asociar una cuenta de correo a una PC en particular de la red interna.

- Debe existir un procedimiento de priorización de mensajes, de manera que los correos electrónicos de prioridad alta sean resguardados.
- Deberá asignarse una capacidad de almacenamiento fija para cada una de las cuentas de correo electrónico de los empleados.
- Deberá utilizarse más de una herramienta antivirus en los servidores, para así disminuir el riesgo de infección.
- Deberán existir discos de rescate de los antivirus, tanto para los futuros servidores como para los puestos de trabajo, que sean capaces de realizar escaneos de virus a bajo nivel y restaurar los sistemas.
- El firewall de la empresa debe presentar una postura de negación preestablecida, configurado de manera que se prohíban todos los protocolos y servicios, habilitando los necesarios.
- Los servicios o protocolos que solo sean necesarios esporádicamente deberán habilitarse on demand. Aquellos que sean considerados riesgosos deberán habilitarse bajo estrictas limitaciones de uso, considerando el equipo desde el que se utilizará, hacia qué destino, las fechas y los horarios para dichas conexiones. A modo de ejemplo, esto puede aplicarse a la utilización del protocolo FTP seguro para la comunicación con las fábricas.
- El encargado de mantenimiento debe controlar periódicamente la configuración del firewall y los servicios de red, documentando los resultados de dichas pruebas.
- De haber una falla en el firewall, debe ser una “falla segura”, lo que significa que todos los accesos al servidor de Internet deben bloquearse.
- Toda la información que se considere confidencial deberá encriptarse durante la transmisión, o viajar en formato no legible.

- Deben existir procedimientos formalmente documentados destinados a prevenir los ataques de red más frecuentes.
- Se deberá usar algún sistema de detección de intrusos (IDS), tolerantes al fallo, utilizando los mínimos recursos posibles.
- Deberá utilizarse una herramienta que monitoree la red, con el fin de evitar el ataque de denegación de servicio (DoS).
- Para disminuir el riesgo de sniffing, la red de la empresa deberá segmentarse física y/o lógicamente.
- Con el fin de disminuir la posibilidad de spoofing el firewall deberá denegar el acceso a cualquier tráfico de red externo que posea una dirección fuente que debería estar en el interior de la red interna.
- Los archivos de passwords y datos de usuarios no deberán almacenarse en el directorio por default destinado a tal fin. Además, deberán estar encriptados utilizando encriptación en un solo sentido ("one way"), con estrictos controles de acceso lógico, de manera de disminuir la posibilidad de ataques.
- El sistema operativo de los servidores deberá presentar las siguientes características:
    - ✓ alta confiabilidad,
    - ✓ equilibrio en costo y beneficio,
    - ✓ compatibilidad e interoperabilidad con los sistemas operativos de las PC´s y demás sistemas usados en la empresa,
    - ✓ escalabilidad,
    - ✓ disponibilidad de software de aplicación y actualizaciones,
    - ✓ buena administración y generación de logs,

- ✓ buena performance,
- ✓ cumplir con los requerimientos funcionales impuestos por la empresa,
- ✓ amigable con el usuario,
- ✓ disponibilidad de documentación.

- Además, deberá presentar las siguientes características en lo relativo a la seguridad:
  - ✓ identificación y autenticación,
  - ✓ control de acceso,
  - ✓ login,
  - ✓ incorruptibilidad,
  - ✓ fiabilidad,
  - ✓ seguridad en la transmisión,
  - ✓ backup de datos,
  - ✓ encriptación,
  - ✓ funciones para preservar la integridad de datos,
  - ✓ requerimientos sobre privacidad de datos.
- El administrador de sistemas deberá confeccionar un Plan de Migración desde archivos indexados a bases de datos relacionales, una vez que el sistema este desarrollado en su totalidad.
- Los archivos indexados de la empresa, las carpetas donde se encuentran almacenados y las aplicaciones que los administran deberán tener controles de acceso, de forma tal que la única persona que pueda tener acceso a estos recursos sea el administrador del centro de cómputos.
- Debe existir una aplicación que registre las siguientes ocurrencias:

- ✓ tiempo y duración de los usuarios en el sistema,
- ✓ número de conexiones a bases de datos,
- ✓ número de intentos fallidos de conexiones a bases de datos,
- ✓ ocurrencias de deadlock con la base de datos,
- ✓ estadísticas de entrada-salida para cada usuario,
- ✓ generación de nuevos objetos de bases de datos,
- ✓ modificación de datos.

- Deberán hacerse chequeos regulares de la seguridad de la base de datos, en los que se deberá verificar que:
  - ✓ se hacen y son efectivos los backups y los mecanismos de seguridad,
  - ✓ no haya usuarios de la base de datos que no tengan asignado una contraseña,
  - ✓ se revisen los perfiles de los usuarios que no han usado la base de datos por un período largo de tiempo,
  - ✓ nadie, además del administrador de datos, ha accedido a los archivos del software de base de datos y ha ejecutado un editor de archivos indexados,
  - ✓ solo el administrador de datos tiene acceso de lectura y escritura en los archivos de programa,
  - ✓ la base de datos y las aplicaciones que la administran tiene suficientes recursos libres para trabajar eficientemente.
- Deben mantenerse registros de todas las transacciones realizadas en la base de datos, de manera que éstas puedan revertirse en caso de surgir un problema. Los registros de la base de datos no se borrarán físicamente, sino que deberán marcarse como eliminados.
- Deberán existir estándares del o los servidores.

- Antes de hacer un cambio en la configuración de los servidores se deberá hacer un backup de la configuración existente. Una vez que el cambio ha resultado satisfactorio deberá almacenarse la configuración modificada.
- Se deberá establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores en el caso de generarse problemas.
- Se deberán realizar chequeos periódicos en los servidores en búsqueda de aplicaciones instaladas no autorizadas o innecesarias.
- Los datos de entrada y salida del sistema deberán poseer controles donde se verifique su integridad, exactitud y validez.
- Los datos de salida del sistema de la empresa deben restringirse con controles lógicos, de acuerdo a los permisos de acceso.
- Deberán protegerse con controles de acceso las carpetas que almacenen los archivos de las aplicaciones, y solo el administrador de sistemas tendrá acceso a ellas.
- Se deberá utilizar un programa de sincronización horaria en todo el entorno de red, para asegurar la consistencia de los datos de las aplicaciones.
- El procedimiento de generación de backup deberá estar automatizado con alguna herramienta de generación de copias de respaldo de datos.
- Deberán realizarse chequeos para comprobar el funcionamiento correcto de los medios externos donde se realizan las copias de respaldo. Además, debe existir una política de reemplazo de medios externos de almacenamiento de backups, de manera de sustituirlos antes de su degradación física, y deberán poseer rótulos que los identifiquen.

- Deben generarse copias de respaldo de las configuraciones de los servidores, documentando las modificaciones realizadas para identificar las distintas versiones. Se deberá establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores

d) Personal Administrativo

- Definir sus responsabilidades y funciones respecto al diseño, establecimiento, control, ejecución y actualización del Plan de Seguridad a través de Capacitación continuas
- Se debe especificar las atribuciones y funciones de las distintas categorías de personal, y reforzando el área de IT que incluyan Jefes y especialistas de informática; Administradores de redes, sistemas y aplicaciones; Especialistas de Seguridad y Protección; Responsables de Seguridad Informática y Usuarios comunes de las tecnologías de Información.

IX. REFERENCIAS BIBLIOGRÁFICAS

1. Albox.com [Internet], Argentina: Citado 20 Nov. 2016 disponible en http://www.albox.com.ar/capacitacion/seguridad_informatica/como_armar_un_plan_de_seguridad_informatica.htm
2. Dspace.espol.edu.ec [Internet],Ecuador: 2006, citado diciembre 2016; disponible en https://www.dspace.espol.edu.ec/bitstream/123456789/15875/1/CICYT.doc
3. icetex.gov.co [Internet], Colombia: Octubre 2014: citado Enero 2017 disponible en https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf
4. e-archivo.uc3m.es [Internet], Madrid: Noviembre 2009: citado Noviembre 2016; disponible en

http://earchivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf?sequence=1

5. stadium.unad.edu.co [Internet], Colombia: 2015; citado Noviembre 2016: disponible en http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3613/3/52761210_60334684.pdf
6. mgd.redrta.org [Internet], España: Enero 2015, citado noviembre 2016; disponible en http://mgd.redrta.org/directrices-seguridad-de-la-informacion/mgd/2015-01-22/145337.html
7. sgs.co [Internet], Colombia. Citado enero 2017; disponible en http://www.sgs.co/es-ES/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx
8. pmg-ssi.com [Internet], actualizado septiembre 2015, citado enero 2017, disponible en http://www.pmg-ssi.com/2015/09/beneficios-iso-iec-27001-2013/
9. dokumentalistas.com [Internet] citado enero 2017, disponible en http://www.dokumentalistas.com/articulos/buenas-practicas-seguridad-informacion-iso-27001/

X. ANEXO

A. Cuestionario Diagnóstico Estado Actual ISO 27001:2013 de PRODUCE

TECNOLOGÍA		Responsable	2016
Electricidad	Validar que el suministro eléctrico de datos siga esquema de instalación recomendado		3.00
	Verificar que todos los elementos de la red de datos estén conectados a tierra (TIA 607 vigente)		3.00
	Determinar el consumo eléctrico de los equipos, segregando por áreas		3.00
	Contar con respaldo ante caída (UPS / Planta Eléctrica)		3.00
	Seguridad física en los páneles de control		4.00
	Pruebas periódicas de caída del suministro externo		0.00
Cableado de Datos	Validar cumplimiento de normas de cableado estructurado (ISO/IEC 24764, EIA/TIA 942/568/569/606/607)		0.00
	Etiquetar cableado para su rápida identificación		0.00

Networking	DIRECCIONAMIENTO IP: Cumplimiento del RFC# 1918		0.00
	DATOS: Balanceo de acceso a Internet (configuración de BGP de ser requerido -- redundancia)		0.00
	DATOS: DHCP Snooping		0.00
	DATOS: Establecer configuraciones de QoS (prioridad gestión de la red)		0.00
	DISEÑO: Redundancia en los enlaces críticos		0.00
	DISEÑO: Segmentación de la red. Restringir tráficos (separar red de los biométricos en las entradas)		0.00
	DISEÑO: Topología en estrella. No cascada. Preferiblemente switches stackeados.		0.00
	DISEÑO: VTP domain		0.00
	DISEÑO: Normalización de los equipos (estandarización)		0.00
	FIREWALL: Configuración de Firewall según políticas (ISO 27002)		0.00
	FIREWALL: Firewall / IPS / IDS actualizado con las últimas firmas		0.00
	FIREWALL: Instalar Firewall / IPS para la inspección del tráfico entrante/saliente. Diseño multi-tier.		0.00
	FIREWALL: Restringir accesos remotos al Firewall (pantalla de inicio -- desde Internet)		0.00
	SEGURIDAD: Actualización de versiones / actualización de infraestructura (parchado)		0.00
	SEGURIDAD: Para equipos Cisco (no usar "password", usar "enable")		0.00
	SEGURIDAD: Gestión segura (SSH). No Telnet		0.00
	SEGURIDAD: Habilitación de DMZ (Servicios/Aplicaciones expuestas a Internet)		0.00
	SEGURIDAD: Hardening routers (ACL, bloqueo de puertos, banner, descripciones, seguridad protocolos routing)		0.00
	SEGURIDAD: Hardening switches (switchport portsecurity, ACL, bloqueo de puertos, banner, descripciones,snmp,login,logging)		0.00
	SEGURIDAD: No repudio. Usuarios no genéricos (todos los equipos de redes y seguridad)		0.00
	SEGURIDAD: Realizar prueba de vulnerabilidades / análisis de penetración		0.00
	SEGURIDAD: Restricción de acceso en los equipos de redes		0.00
	SEGURIDAD: Validar comunicación VPN en el negocio (interna, con terceros, socios). Accesos restringidos		0.00
	SEGURIDAD: Trazabilidad de las transacciones (audit logs)		0.00
	SEGURIDAD: Protección de roles "admin" "administrator" "superuser"		0.00
	SEGURIDAD: Implementar un DLP Corporativo		0.00
	VOZ: Configuración segura de teléfonos (hardening)		0.00
	WEBFILTER: Bloquear descargas de .zip, .exe, .rar sin autorización		0.00
	WEBFILTER: Bloqueo de categorías "no permitidas" por defecto		0.00
	WIFI: Bloqueo de WPS		4.00
	WIFI: Conocer la cobertura Inalámbrica (evitar "warwalking")		0.00
	WIFI: Seguridad / Control de acceso y gestión para el WLC		0.00
	WIFI: SSID no evidentes (Capacitación, PDT, Proveedores, Scales, USERS, Verificadores)		0.00
	WIFI: Segmentar redes según target. DMZ de ser requerido		0.00
	WIFI: Todas las redes deben operar en WPA-2 Personal / Enterprise (AES)		4.00

Servidores	Aplicar Hardening a los servidores (bloqueo de puertos no necesarios, parchado/actualización)		0.00
	VLAN de intercomunicación entre servidores, debe ser diferente a la VLAN de usuarios		0.00
	Servicio seguro de transferencia de archivos (sFTP)		0.00
	Servidores no deben ir conectados en un switch que comparta acceso con los usuarios finales		0.00
	Definir matriz de perfiles y derechos, activarlo en Active Directory		0.00
	Creación de perfiles de usuario (a partir del básico)		0.00
	Protección de roles "admin" "administrator" "superuser"		0.00
	RDP seguro (NLA)		0.00
	Gestión segura (SSH). No Telnet		0.00

Aplicaciones	Definir e implantar una metodología ágil de desarrollo		0.00
	Privacidad de la información. No exponer data sensitiva. Cifrado de datos base de datos		0.00
	Trazabilidad de las transacciones (audit logs)		0.00
	Restringir acceso de aplicaciones críticas, basado en la matriz de perfiles y derechos definidos en Active Directory		0.00
	Protección del Código Fuente		0.00
	Configuraciones por defecto (páginas de inicio por defecto)		0.00
	Separación y aplicación de seguridad para ambientes de desarrollo / pruebas / producción		0.00

Aplicaciones Web	Implementación de WAF		0.00
	Compra de dominios similares (no sólo .com, también .net, .info, .co)		0.00
	Renovación de dominios programados anualmente - Reputación		4.00
	Certificados digitales (recomendación Digicert costo / beneficios)		0.00
	Restricciones de acceso. Restringir visibilidad de pantallas de gestión del sitio (e.g. wp-admin en Wordpress)		4.00
	Realizar un análisis de vulnerabilidad basado en la OWASP		0.00
	Página Principal -- Seguridad en Formularios, subir archivos .exe		0.00
	Configuraciones por defecto (páginas de inicio por defecto)		4.00
	Restricción por IP. Acceso o visibilidad sólo del personal que lo requiere		0.00
	Hosting del sitio principal. Respaldo y tiempo de resolución frente a un incidente		2.00

Base de Datos	Password almacenados cifrado		0.00
	Firewall de Base de Datos (SQL & Oracle)		0.00
	Buenas prácticas de configuración (ambiente desarrollo / prueba / producción)		0.00
	Pasar los datos confidenciales actuales a una tabla aparte. En la tabla original, enmascarar la información		0.00
	Crear una rutina única de acceso y modificación de la tabla de datos confidenciales		0.00
	Seguridad "Especial" - Base de Datos		0.00
	Respaldo Base de Datos -- página principal		0.00
	Protección de roles "admin" "administrator" "superuser"		0.00
	Protección de datos utilizados en ambientes de prueba y calidad		0.00
	Almacenamiento de información de tarjetas de créditos de clientes		0.00
	Trazabilidad de las transacciones (logs)		0.00

Correo Electrónico	Antispam --- alternativa para Office 365???		0.00
	Comunicación cifrada entre correos TLS 1.2		0.00
	Acceso Web (permisos) - restringir su uso		2.00
	Activar servicio DLP (Office 365)		0.00
	Respaldo de Correos (restauración). Retención de correspondencia (aspecto legal)		0.00
	No permitir el envío/descarga de archivos de extensión riesgosas / tamaño muy grande		2.00

Dispositivos de Acceso Fijos (PC)	Definir un plan de renovación de hardware y upgrade de sistemas operativos (por perfil de usuario)		0.00
	No abrir MACROS por defecto (aplicable a todos los software de Ofimática)		2.00
	Almacenamiento de la información respaldado		3.00
	Puertos USB Bloqueados		2.00
	Uso de USB con software de cifrado		2.00
	Actualización / parchado		0.00
	Políticas de Navegación		0.00
	Bloqueo automático de sesiones / pantallas (equipos sin atención)		0.00
	Bloqueo por intentos fallidos		0.00
	RDP seguro (NLA)		0.00
	Uso sólo de software autorizados - licenciados / no crack (riesgo de demandas, allanamientos)		0.00
	Instalación de vacuna ransomware		0.00
	Permisos de Administrador / Instalación de Software		0.00
	Especial Atención a Sitios Públicos Expuestos (Atención al Cliente)		0.00
	LAPTOP: Cifrado de discos (prevención en caso de robos, pérdidas)		2.00
	Administración de seguridad en correos y datos confidenciales (recomendación: recursos en la nube)		0.00

Dispositivos de Acceso Móviles (Laptops / Celulares / Tablets / Terminales de Tarjetas)	Segmentación Área Negocios - Datos Personales		2.00
	Control Remoto - Borrado de información de dispositivos móviles (celulares)		0.00
	Permisos - restricciones		0.00
	Uso de WiFi-- Acceso a nuestra red		4.00
	Antivirus actualizado		4.00
	Mensajería Instantánea Segura -- Threema / Telegram		3.00
	Manejo seguro de correo electrónico (workplace - e.g. Airwatch)		3.00
	Manejo de documentos descargados (workplace - e.g. Airwatch)		0.00
	Bluetooth desactivado		4.00
Impresoras	Código de impresión por usuario		0.00
	Cableadas o inalámbricas. Validar seguridad y segmentación		0.00
	Restringir accesos remotos (configuraciones)		0.00

Monitoreo	Implementación de SIEM (networking, servidores, aplicaciones, base de datos)		0.00
	Debida configuración de un NTP server. Todos los equipos apuntando a este dispositivo		0.00
	Retención de logs - 90 días (en caso de forensia digital)		0.00
	Sensores de Data Center. Alertas / notificación por correo		0.00
	Implementación de un NAC		0.00
	Definir un Baseline (salud de la red). Determinación de comportamiento erráticos (definición de thresholds)		0.00
	Monitoreo proactivo de la salud de la red y sus componentes (Nagios, Cacti)		0.00
	Micrófonos escondidos / salones de conferencias		0.00
	Implementación de APT monitor/detection		0.00
	Implementación de IPS/IDS. Firmas actualizadas		0.00

PROCESOS		Control ISO 27001	Responsable	Costos	2016
Gestión de la Información	Definir e implantar un esquema de gestión de riesgo operacional tecnológico	A12			2.00
	Definir e implantar un Sistema de Gestión de Seguridad de TIC (27001-2). Publicar políticas de seguridad	A5			2.00
	Revisión periódica de las políticas de seguridad para asegurar su efectividad y cumplimiento	A5			0.00
	Establecer la identificación, almacenamiento, movilización y acceso de la información de la empresa	A8			0.00
	Clasificación de la información	A8			0.00
	Evaluar escenario posible para aplicar la técnica "split-knowledge"	A9			0.00
	Programa SETA (Security Education, Training and Awareness)	A7			0.00
Service Desk	Definir e implantar procesos de Service Desk	A16			0.00
Oferta y Acuerdos de Servicios	Firma de NDA / Acuerdo de Confidencialidad con proveedores y colaboradores	A7			0.00
	Definir e implantar proceso para la gestión de niveles de servicio (disponibilidad y soporte)	A17			0.00
Transición	Definir e implantar proceso para la gestión de cambios	A12			0.00
	Definir e implantar proceso para la gestión de activos y configuración	A8			0.00

Manejo de Procesos de Seguridad Fundamentales	Inducción al usuario sobre la manejo de la información confidencial de los clientes	A7			3.00
	Proceso de contratación del personal. Inducción del personal en temas de seguridad	A7			3.00
	Gestión del personal, de forma segura, mientras esté bajo contrato. Procesos disciplinarios	A7			3.00
	Proceso de renuncia/despido del personal	A7			0.00
	Políticas para el desecho de documentación física (trituración de papel)	A8			0.00
	Política de cambio periódico de contraseñas (incluyendo las de mercadeo digital)	A9			4.00
	Política de "Escritorios Limpios"	A11			3.00
	Política de "Uso Aceptable" de los recursos corporativos	A8			0.00
	Políticas para el desecho tecnológico (formateo / destrucción física de dispositivos de almacenamiento masivo)	A8			0.00
	Respaldo/Backup de la información (retención de data ?años?). Pruebas de restore	A12			4.00
	Políticas para definir el mínimo de seguridad en la estructura de Password / Passphrases	A9			4.00
	Política para reparación de computadoras por proveedores externos	A8			3.00
	Procedimientos para escalar incidentes y/o fallas	A16			0.00
	Política de Entrada / Salida de Activos	A8			0.00
	Política de Retorno de Equipos (laptops, celulares)	A8			0.00
	Almacenamiento de la información (retención de data)	A18			3.00
	Procedimiento para el manejo de incidentes de seguridad	A16			0.00
	Definir controles en áreas de carga y descarga de activos	A11			0.00
	Procedimiento para atención de computadoras infectadas (malware)	A12			0.00
	Definir procedimientos internos para mantenimiento adecuado del cableado	A12			0.00
	BCP / DRP documentados y probados regularmente	A17			0.00
	Políticas definidas para BYOD	A6			0.00
Certificaciones Corporativas	Certificarse ISO 27001:2013	A5			0.00
	Certificarse PCI DSS	A18			0.00

PERSONAL		Control ISO 27001	Responsable	Costos	2016
Personal TIC	Reorganizar la unidad TIC (enfoque seguridad)	A6			2.00
	Mapa de capacitación del personal	A6			0.00
	Acceso al área de IT Restringido	A11			0.00
	Rotación de roles / redundancia / segregación de roles y funciones	A6			0.00
	Clima organizacional	A6			2.00
	Contratar a un Oficial de Seguridad de la Información (recomendación forme parte de IT)	A5			0.00
Personal en General	Revisión de la estructura organizacional por área / mercado	A6			0.00
	Evaluar la documentación de roles y funciones	A6			0.00
	Evaluar permisos / autorizaciones de proveedores (e.g. empacadores, personal de limpieza, despachadores)	A6			0.00

DOCUMENTACIÓN		Control ISO 27001	Responsable	Costos	2016
Tecnología	Diagrama de los panales de distribución	A11			0.00
	Diagrama de conexión del sistema de respaldo de fluído eléctrico	A11			0.00
	Diagramas unifilares del tendido de cables de poder	A11			0.00
	Tablas de distribución de carga en función del consumo eléctrico de los equipos conectados	A11			0.00
	Diagrama general de cableado estructurado por localidad	A11			0.00
	Diagrama del cableado horizontal	A11			0.00
	Diagrama de conexión de servidores	A13			0.00
	Conectorización por rack de equipos a patch panel	A11			0.00
	Diagrama físico de la red	A13			3.00
	Diagrama lógico de la red	A13			3.00
	Configuración de equipos de comunicaciones (respaldo)	A12			0.00
	Baseline del comportamiento de la red	A16			0.00
	Inventario de equipos de comunicaciones (incluyendo inalámbrico)	A8			4.00
	Inventario de direccionamiento IP	A8			4.00
	Localización geográfica de los centros de datos	A11			0.00
	Diagrama de distribución de racks	A13			0.00
	Cálculo de RLUs en los racks	A13			0.00
	Diagramas de distribución de espacio horizontal y vertical	A11			0.00
	Diagramas del sistema HVAC en los centros de datos	A11			0.00
	Diagramas del sistema contra incendio en los centros de datos	A11			0.00
	Inventario de equipos del centro de datos	A8			0.00
	Inventario físico de servidores	A8			0.00
	Lista de servidores virtuales por servidor físico	A8			0.00
	Configuración base de los servidores (respaldo)	A12			0.00
	Listado de procesos activos en los servidores	A8			0.00
	Relación Servicios - Servidores - Aplicaciones	A14			0.00
	Diagramas provistos por la metodología de desarrollo de software utilizada: BDA, modelo datos, DFD	A14			0.00
	Inventario de aplicaciones (de escritorio, Web y SAP)	A8			4.00
	Listado de aplicaciones permitidas / autorizadas	A12			4.00
	Inventario de dispositivos (PC, laptops, tablets, PDT, POS, Pesas, celulares, cajas, impresoras)	A8			4.00
	Listado de personal con autorización para ver correo vía Web	A6			4.00

Procesos	Políticas	**A5**			2.00
	Normas	**A5**			2.00
	Procesos	**A5**			2.00
	Procedimientos de seguridad	**A5**			2.00
	Procedimientos de operativos	**A12**			2.00
	Guías	**A5**			0.00
	Indicadores	**A5**			0.00
	Herramientas de análisis	**A16**			0.00
	Contratos / NDA / SLA	**A7**			0.00
Personal	Curriculum actualizado	**A7**			0.00
	Matriz de competencias	**A7**			0.00
	Plan de educación	**A7**			0.00
	Organización interna	**A6**			3.00
	Descripciones de cargos, roles y funciones	**A6**			3.00

B. Imágenes de Equipo de Contabilidad

Se utiliza una torre como servidor de Peachtree, esta es una parte esencial dentro de la sociedad a mejorar.

Figura. 5 Servidor de Peachtree