DESARROLLO E IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA A LA CAJA DE PREVISIÓN SOCIAL DE LA UNIVERSIDAD DE CARTAGENA

CARLOS ALFONSO LARA OROZCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CARTAGENA DE INDIAS D.T. Y C.
2015

DESARROLLO E IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA A LA CAJA DE PREVISIÓN SOCIAL DE LA UNIVERSIDAD DE CARTAGENA

CARLOS ALFONSO LARA OROZCO

Tesis de grado para optar por el título:
Especialista En Seguridad Informática

Director de Proyecto:
Ing. Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CARTAGENA DE INDIAS D.T. Y C.
2015

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, 31 de Mayo de 2015

DEDICATORIA

A mis padres y hermanos que siempre han estado para apoyar cada uno de los pasos que doy hacia mi crecimiento personal y profesional. Y de forma especial, a mi esposa y a mi hijo, que ahora son mi nuevo motor.

AGRADECIMIENTOS

A cada miembro de mi familia, que tuvieron que ceder nuestro tiempo destinado a compartir para que culminara este peldaño más en mi vida profesional.

A la Caja de Previsión Social de la Universidad de Cartagena por permitir la realización de este proyecto, así como cada una de las personas que laboran en ella y que fueron determinantes para la realización de este proyecto.

A cada uno de los docentes y compañeros que compartieron conmigo en cada una de las asignaturas que comprenden esta especialización, así como también a la directora de proyecto, Erika Villamizar Torres, por dedicarle todo el tiempo posible y estar muy pendiente del avance y culminación del presente trabajo.

CONTENIDO

pág.

LISTADO DE TABLAS

pág.

LISTADO DE FIGURAS

pág.

LISTA DE ANEXOS

RESUMEN

El presente proyecto se centra en la elaboración e implementación de un manual de políticas de seguridad informática para la Caja de Previsión Social de la Universidad de Cartagena, basándose en la ISO/IEC 27002:2013, norma que establece los dominios y controles para obtener la seguridad de la información de cualquier empresa u organización. Para esto es necesario realizar un análisis de riesgos a los cuales se encuentra expuesta la entidad y con base en el resultado del mismo, establecer las políticas que permitirán reducir riesgos y vulnerabilidades al tiempo que aumenta la seguridad, siempre y cuando haya un total compromiso de las directivas en su implementación y puesta en marcha, capacitando de manera constante al personal involucrado y efectuando pruebas para verificar la efectividad de las políticas. Es necesario realizar de manera permanente, de acuerdo a lo establecido, actualizaciones de dichas políticas debido a que los sistemas de información y la legislación tienden a ser cambiantes, así como también las vulnerabilidades y riesgos que puedan surgir después de la elaboración del manual resultado del presente proyecto.

Palabras claves: Políticas de seguridad de la información, riesgos, vulnerabilidades, ISO/IEC 27001:2013, ISO/IEC 27002:2013, confidencialidad, integridad, disponibilidad, seguridad.

INTRODUCCIÓN

Actualmente todo tipo de organización maneja datos de vital importancia para el funcionamiento de la misma, utilizando sistemas de información que permiten su correcto procesamiento y posterior almacenamiento. El utilizar dichos sistemas implica el uso de equipos y redes de datos que se encarguen de la transmisión de los mismos entre los servidores y cada uno de los usuarios que acceden a ellos. Este traslado de información provoca la aparición de vulnerabilidades, poniendo en riesgo todo el sistema informático.

Es por ello, que se debe buscar la mejor manera para mantener de forma segura todos los datos sensibles de la entidad, siendo una tarea continua y de gran importancia, ya que conforme pasa el tiempo son más las personas que buscan acceder de forma fraudulenta a los sistemas de información empleando cada vez nuevas técnicas de infiltración, pudiendo todos estos ataques originarse desde fuera de la entidad así como desde dentro de la misma. Para ello, es muy importante que si se quiere disminuir de forma exponencial cualquier probabilidad de pérdida o escape de información sensible, es necesario establecer un manual de políticas de seguridad informática en el que se establezcan pautas a seguir por cada uno de los empleados.

La Caja de Previsión Social de la Universidad de Cartagena es una entidad encargada de prestar servicios médicos y asistenciales a los docentes, empleados, jubilados y beneficiarios de los mismos, encaminada en un proceso de acreditación de la calidad pero que, no cuenta con un sistema de seguridad para la información que en ella se procesa.

De a lo anterior, este proyecto generará las políticas de seguridad informática deben ser diseñadas a la medida para la Caja de Previsión Social de la Universidad de Cartagena, describiendo claramente qué y por qué se desea proteger y así mismo concientizar al personal en el cumplimiento y el acato de estas políticas.

1. DESCRIPCIÓN DEL PROBLEMA

La Caja de Previsión Social de la Universidad de Cartagena, es una entidad aseguradora y prestadora de servicios de salud a los empleados activos y jubilados de la Universidad de Cartagena, la cual, con el paso del tiempo ha ido adaptándose a los cambios en cuanto sistemas de información se refiere, cumpliendo con las normatividades que rigen el área de la salud, dejando de lado aspectos importantes como la seguridad informática, la cual permite proteger todos los recursos del sistema de información de cualquier institución u organización, desde la parte física hasta cada uno de los datos que son transmitidos a través del mismo, asegurando además que la información sea accedida en el momento que se necesite por las personas autorizadas para ello, evitando que sea alterada, robada o eliminada, todo esto con el fin de asegurar la confidencialidad, integridad y disponibilidad de dicha información.

Algunas auditorías realizadas en la Caja de Previsión por entes territoriales han evidenciado que no se tienen implementados mecanismos de seguridad informática, al ver que la mayoría de los empleados utilizaban el mismo usuario y contraseña para acceder al sistema de información, con el agravante de que dicho usuario posee todos los privilegios. Otro problema es el hecho de que no hay un software antivirus que impida la infección por todo tipo de virus o malware que se propagan a través de correos electrónicos como spam, por el uso de dispositivos extraíbles, etc.; estas vulnerabilidades ponen en riesgo cada uno de los elementos que pertenezcan a la red, incluyendo los servidores que son la base del sistema de información.

Pasando al aspecto físico, es notoria la carencia de seguridad ya que el acceso al área de Sistemas no cuenta con cerraduras efectivas ni cámaras de seguridad, además no posee mecanismos de prevención ni detección, es decir, cualquier persona puede llegar a dicha área sin inconvenientes y no ser descubierto, pudiendo atentar en todos los aspectos a la seguridad del sistema de información. Tampoco se cuenta con planes de contingencia en caso de presentarse cualquier tipo de calamidad que afecten la disponibilidad, desde averías de pequeñas piezas, pasando por daños en los equipos que requieran un cambio completo del mismo y llegando a desastres por causas naturales como terremotos e inundaciones.

Dado que se cuenta con una sola persona para la realización de lo debido en dicha área, no ha sido posible establecer suficientes mecanismos para lograr una seguridad óptima en dicha oficina.

La Caja de Previsión Social de la Universidad de Cartagena, debería iniciar a implementar un sistema de seguridad informática debido a que se encuentra en un proceso de acreditación y habilitación, para lo cual las políticas de seguridad informática le serán de gran apoyo para dicho proceso. Además de esto, es factible que en cualquier momento la entidad pueda ser víctima de un ataque o delito informático, impidiendo su normal funcionamiento.

2. FORMULACIÓN DEL PROBLEMA

¿De qué manera se pueden aumentar los niveles de seguridad, en el ámbito de la información y todos los recursos tecnológicos de la Caja de Previsión Social de la Universidad de Cartagena?

3. JUSTIFICACIÓN DEL PROYECTO

La información en las entidades, representa un recurso que ha ido aumentando de importancia en la medida en que se utilizan los sistemas de información para el procesamiento de la misma.

En la Caja de Previsión, se han implementado normas concernientes al área de la salud, ya que esta es su misión, adquiriendo equipos y software que le permitan prestar un buen servicio; pero se ha dejado de lado lo relacionado con la seguridad de la información que allí se maneja, pudiendo ser objeto de todo tipo de amenazas que afecten la confidencialidad, integridad y disponibilidad.

Un tipo de información que se procesa en la entidad es una Historia Clínica, que como lo establece la Resolución 1995 de 1999 en el Capítulo I Artículo 1 “es un documento privado, obligatorio y sometido a reserva (…)”, y esta solo debe ser vista por el (los) médico(s) tratante(s) y por el mismo paciente, evitando que terceros o extraños acceda a ella para tomar provecho de esta o que sea modificada; además, si estos o los demás datos que la entidad maneja llegaran a fallar o si se presenta algún daño en la infraestructura tecnológica, los usuarios quedarían sin acceso al sistema de información impidiendo la atención oportuna de los pacientes que se atienden durante todos los días de la semana.

Las medidas de seguridad establecidas en cualquier organización deben ser aplicadas sin importar la forma en que sean almacenados los datos, como se procesan o transmiten, incluyendo controles de acceso basado en niveles de acuerdo a las funciones de cada usuario.

La norma ISO/IEC 27002:2013 establece 11 dominios y controles para cada uno de ellos, siendo el primer dominio la “Política de seguridad de la información”, la cual consta de 2 controles: “Documento de política de seguridad de la información” y “Revisión de la política de seguridad de la información”; aspectos de vital relevancia para la finalidad de este proyecto, que consiste en estructurar un buen manual donde se proporcionen instrucciones claves sobre la protección de la información de la entidad y los elementos que para ella funcionan, como servidores, dispositivos de red, computadores, etc., generando conciencia en los trabajadores para su debido cumplimiento y estableciendo medidas disciplinarias por la violación de las normas impartidas, porque “si no hay conocimiento y compromiso por parte de todos los actores, estas políticas no producirán ningún efecto benéfico”[1].

[1] Castaño Galvis, W., & González Sanabria, Y. A. (2012). FUNDAMENTOS DE SEGURIDAD DE LA INFORMACION. Bucaramanga: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, p. 37

4. OBJETIVOS DEL PROYECTO

4.1 GENERAL

Elaborar e implementar un Manual de Políticas de Seguridad Informática para resguardar la información que se utiliza en la Caja de Previsión Social de la Universidad de Cartagena, utilizando la norma ISO/IEC 27002:2013.

4.2 ESPECÍFICOS

- Realizar un estudio preliminar sobre la situación de la seguridad informática actual de la Caja de Previsión Social de la Universidad de Cartagena, con el fin de establecer los riesgos a los cuales se encuentra expuesto el sistema de información.

- Redactar el manual de políticas de seguridad con base en los hallazgos obtenidos y en los controles establecidos en la norma ISO/IEC 27002:2013 para el dominio de Política de seguridad de la información, estableciendo las pautas que disminuirán las vulnerabilidades.

- Poner en marcha las políticas de seguridad en la entidad, y darlas a conocer a los empleados mediante capacitaciones con el fin de crear conciencia de su estricto cumplimiento.

- Efectuar diversas pruebas de seguridad en las que se pongan a prueba las políticas, así como el cumplimiento de las mismas por parte de los empleados, determinando su efectividad y posibles mejoras.

5. MARCO REFERENCIAL

Al implementar el manual de políticas de seguridad de la información y con el cumplimiento de las mismas minimizaron los riesgos asociados a los activos, fuga de información y pérdidas económicas, originados por la carencia de las normas y políticas de seguridad de la información.

5.1 MARCO TEÓRICO

En la actualidad, todas las organizaciones utilizan la información como un insumo base para la toma de decisiones, siendo ésta producto de las operaciones realizadas por cada una de sus áreas. Debido a su importancia, habrá personas ajenas que intenten obtenerla con fines perjudiciales, que cada día incrementan sus habilidades para poder penetrar las defensas establecidas y lograr hacer algún tipo de daño.

Como respuesta a estas actividades ilícitas, los encargados de custodiar la información organizacional deben desarrollar procesos de seguridad a los sistemas informáticos, creando una barrera protectora que impida el acceso no autorizado a dicha información, así como también sistemas de detección en caso de que terceros logren atravesar o romper los controles establecidos.

La seguridad informática, tiene como uno de sus objetivos principales brindar un alto nivel de resguardo de los datos, partiendo desde un manual de políticas y

normas de seguridad para que cada uno de los empleados las cumpla a cabalidad y así reducir enormemente los riesgos de un ataque tanto interno como externo.

La RFC 1244 define Política de Seguridad como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán"[2]. Dicho de otra manera, es un documento donde se describe qué y por qué se desea proteger, asignando responsabilidades y sanciones por las faltas cometidas; incluyendo los principios de seguridad como son la confidencialidad, integridad y disponibilidad.

5.2 MARCO CONCEPTUAL

- Seguridad de la información: consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización.

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

[2] Borghello, C. (2009). Políticas de Seguridad de la Información. Recuperado el 4 de Diciembre de 2013, de Segu.Info: http://www.segu-info.com.ar/politicas/polseginf.htm

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- Vulnerabilidad: Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CID) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

    - ✓ Permitir que un atacante ejecute comandos como otro usuario
    - ✓ Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
    - ✓ Permitir a un atacante hacerse pasar por otra entidad
    - ✓ Permitir a un atacante realizar una negación de servicio

5.3 MARCO LEGAL

Ley 647 de 2001: La cual se modifica el inciso 3° del artículo 57 de la Ley 30 de 1992, en el que establece el carácter especial del régimen de las universidades estatales u oficiales, pudiendo organizar su propia seguridad social en salud.

Resolución 1995 de 1999 del Ministerio de Salud: Debido a que la entidad en la que se realiza este proyecto funciona como Entidad Promotora de Salud e Institución Prestadora de Servicios al tiempo, debe tenerse en cuenta la Resolución 1995 de 1999 “Por la cual se establecen normas para el manejo de la Historia Clínica” establece que ésta “es un documento de vital importancia para la prestación de los servicios de atención en salud y para el desarrollo científico y

cultural del sector” y también en su artículo 1. define que “La Historia Clínica es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley”.

Ley 1273 de 2009: la cual establece un nuevo bien jurídico denominado “De la protección de la información y de los datos”, en la que se definen penalidades para los delitos informáticos, los cuales atentan contra la confidencialidad, integridad y disponibilidad de los datos y los sistemas de información.

Ley Estatutaria 1581 de 2012: Conocida como la Ley de “Habeas Data”, instituye el derecho constitucional que tienen cada una de las personas a conocer toda la información que se haya recopilado sobre ellas en alguna base de datos o cualquier otro tipo de archivo, así como también obliga a proteger cada uno de esos datos durante su tratamiento.

Decreto 1377 de 2013: Reglamenta parcialmente la Ley de "Habeas Data", por la cual se dictan disposiciones generales para la protección de datos personales.

6. MARCO CONTEXTUAL

6.1 DESCRIPCIÓN DE LA EMPRESA[3]

6.1.1 Reseña Histórica. La Caja de Previsión Social de la Universidad de Cartagena, ha sido la entidad encargada de prestar los servicios médicos y asistenciales a los Docentes, Empleados Administrativos, Trabajadores oficiales, Pensionados, Jubilados y Sustitutos de Pensión de la Universidad de Cartagena que eran atendidos inicialmente por la Caja Departamental de Previsión de Bolívar. Mediante ordenanza No. 033 expedida por la Honorable Asamblea del Departamento de Bolívar son separados el personal docente y administrativo de la Universidad de Cartagena de la Caja Departamental de Previsión. El Acuerdo 75 del 10 de diciembre de 1968 emanado del Consejo Directivo de la Universidad de Cartagena "Por medio del cual se fijan los Estatutos de la Caja de Previsión de la Universidad de Cartagena" procedieron a crear lo que se denominó LA CAJA DE PREVISIÓN SOCIAL DE LOS EMPLEADOS Y OBREROS DE LA UNIVERSIDAD DE CARTAGENA. En 1969, mediante la Resolución 0301 de Mayo 13 de 1.969 emanada de la Gobernación del Departamento de Bolívar, se reconoció la Personería Jurídica de la entidad. En el año 1996 la entidad se adaptó al Sistema General de Seguridad Social, dispuesto en la Ley 100 de 1.993. La Caja de Previsión Social de la Universidad de Cartagena, es actualmente una Entidad Especializada de conformidad con lo establecido por el Acuerdo 29 Bis del 10 de octubre de 2.001 "Por el cual se ratifica en la Caja de Previsión Social de la Universidad de Cartagena, la Organización, Dirección, Administración y Funcionamiento del Sistema propio de Seguridad Social en Salud de la

[3] QUIENES SOMOS [En línea], <http://cajaprev.gov.co/?e=quienessomos> [Citado en 17 de Abril de 2015].

Universidad de Cartagena, de conformidad con lo consagrado en el artículo 2do. de la Ley 647 de 2.001".

6.1.2 Misión. Somos la Entidad del Régimen Especial del Sistema Universitario en Salud de la Universidad de Cartagena, administradora y prestadora de servicios de salud que trabaja para brindar a sus usuarios una atención con calidad y eficiencia, enfocados en el bienestar integral de sus usuarios generando impacto positivo en la salud de los mismos, bajo la ética y sentido humanizado aplicando el uso óptimo de los recursos y la capacidad instalada, apoyados con personal idóneo y avances tecnológicos para contribuir con el mejoramiento de la salud de los usuarios.

6.1.3 Visión. Seremos en el año 2.015 la entidad líder en el aseguramiento y prestación de servicios de salud dentro del Sistema Universitario estatal de la Región Caribe, enfocados en el usuario y su grupo familiar, que garantice el autocuidado de su salud para lograr el mejoramiento de la calidad de vida.

6.1.4 Valores.

- Honestidad
- Justicia
- Responsabilidad
- Tolerancia
- Respeto
- Compromiso
- Solidaridad
- Transparencia

- Sentido de pertenencia
- Probidad
- Trabajo en equipo
- Libertad

6.1.5 Propósitos.

- Eficiencia
- Efectividad
- Sostenibilidad
- Calidad
- Continuidad

6.1.6 Política de calidad. La Caja de Previsión Social de la Universidad de Cartagena en cumplimiento de su objeto social y requisitos legales está comprometida con el mejoramiento continuo de sus procesos, proporcionando los recursos necesarios y adecuados para prestar los servicios de salud orientados a la excelencia y satisfacción de sus usuarios a partir del compromiso, sentido de pertenencia y un alto valor ético de sus funcionarios.

6.1.7 Objetivos de calidad.

- Implementar, desarrollar y mantener los sistemas de gestión de la Caja de Previsión Social de la Universidad De Cartagena.

- Optimizar el uso de los recursos de la organización.

- Garantizar a los usuarios una atención cálida, oportuna, accesible y segura, fortaleciendo y monitoreando los servicios de salud prestados por la institución y de su red prestadora.

- Fomentar una cultura de mejoramiento continuo, en un ambiente adecuado de trabajo.

- Asegurar la continua actualización, mantenimiento y seguridad de la información, optimizando los medios necesarios para la operación del día a día.

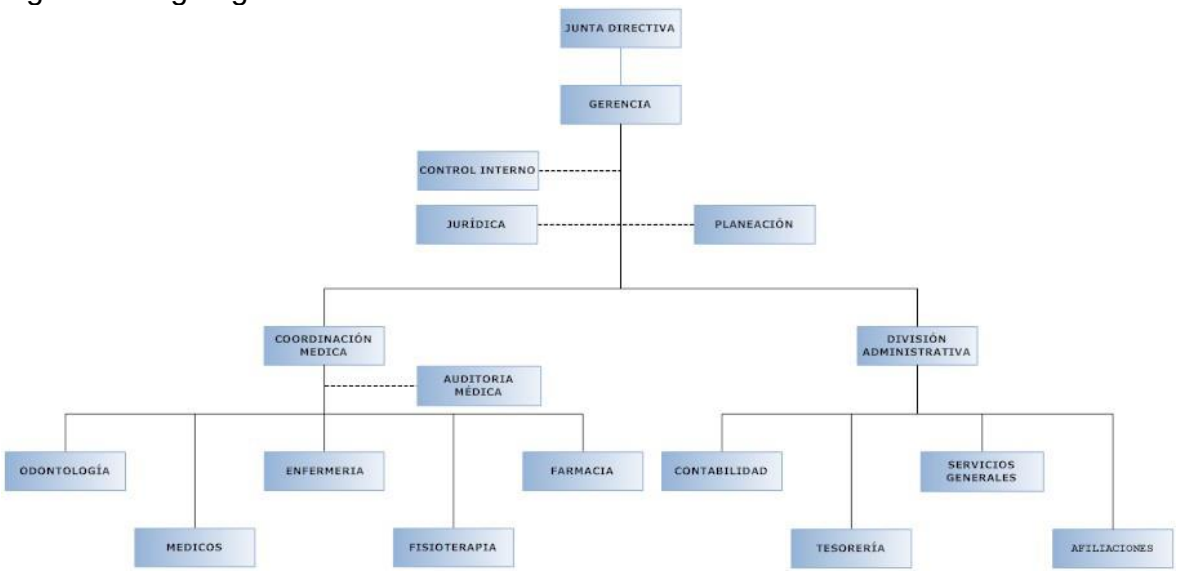
- Fomentar la capacitación y el desarrollo del talento humano.

- Incorporar e implementar tecnologías adecuadas para el desarrollo de la organización.

- Desarrollar e implementar la autoevaluación en todos los procesos de la caja de previsión social de la universidad de Cartagena, con el fin de identificar oportunidades de mejora.

6.1.8 Organigrama. La siguiente figura ilustra el organigrama de la entidad:

Figura 1. Organigrama



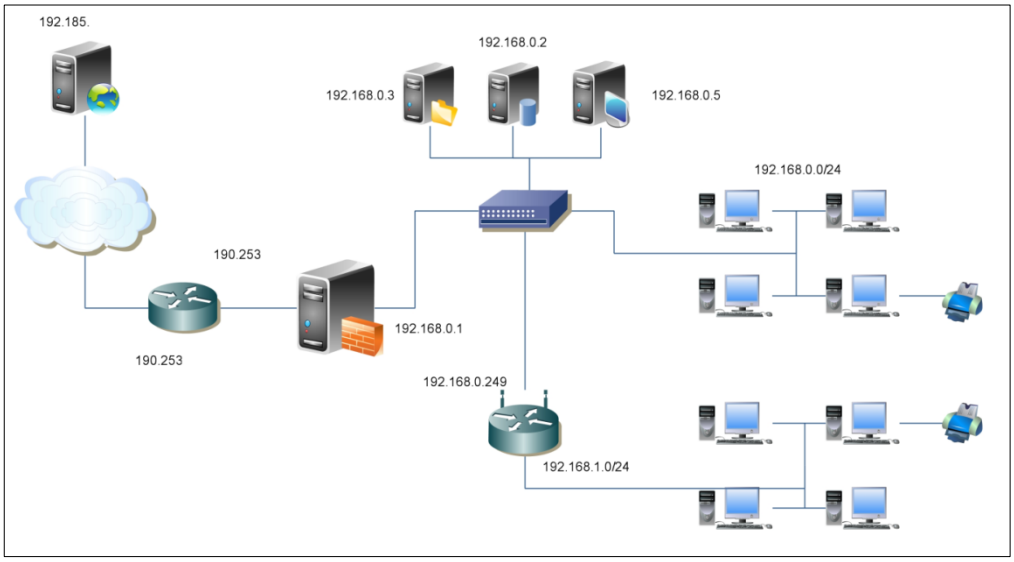
Fuente: Oficina de Sistemas – Caja de Previsión Social de la Universidad de Cartagena

La Caja de Previsión Social de la Universidad de Cartagena cuenta con una Junta Directiva como máximo órgano de la entidad, conformada por un representante de cada uno de los estamentos que hacen parte de la Universidad de Cartagena, como son: Empleados públicos no docentes, Pensionados públicos no docentes, Docentes, Docentes pensionados, Trabajadores Oficiales, Pensionados Oficiales, así como también el Rector de la Universidad como presidente. Dicha Junta Directiva, realiza el nombramiento del Gerente, el cual es el representante legal y ordenar del gasto.

En el momento en que fue creada la entidad, no se tuvo en cuenta la importancia de tener una oficina de Sistemas, por lo que en su organigrama no existe dicha dependencia, pero a medida que la entidad ha ido creciendo se vio la necesidad de crearla, aunque no ha sido modificado el organigrama para incluirla.

6.1.9 Mapa de red. Esta entidad posee una red cableada con un solo switch detrás de un firewall, en el cual están conectados 3 servidores, además hay un router para la red inalámbrica del área administrativa. Los equipos de la red están identificados por una dirección IP local del rango 192.168.0.0/48, mientras que para la salida a internet se utiliza una dirección IP pública.

Figura 2. Mapa de red



Fuente: Oficina de Sistemas

6.1.10 Procesos internos de seguridad en la Oficina de Sistemas. La Caja de Previsión Social de la Universidad de Cartagena, cuenta con una oficina de Sistemas, en la que hay un (1) ingeniero de sistemas encargado de realizar todo lo necesario para el área, desde el mantenimiento preventivo y correctivo de los equipos de cómputo hasta la administración de los servidores.

6.1.11 Necesidades en la Oficina de Sistemas. Dado que no hay suficiente personal para la realización de lo debido en dicha área, no se han establecido

suficientes mecanismos para lograr una seguridad óptima en dicha oficina; para la parte física, no cuenta con cerraduras efectivas ni cámaras de seguridad y por la parte lógica, cuenta con un servidor proxy que funciona también como firewall, encaminando todas las conexiones desde y hacia a internet a través del mismo, filtrando las no deseadas o que no cumplan con los requisitos establecidos previamente.

7. METODOLOGÍA PRELIMINAR

7.1 TIPO DE INVESTIGACIÓN

Este proyecto se realizará siguiendo los lineamientos de una investigación de tipo exploratorio, debido a que en la Caja de Previsión Social de la Universidad de Cartagena, nunca se han realizado este tipo de estudios ni proyectos, enfocados a la creación o aumento de la seguridad informática.

7.2 POBLACIÓN

La población objeto de estudio, es la Caja de Previsión Social de la Universidad de Cartagena, la cual cuenta con un total de 40 empleados.

7.3 MUESTRA

Utilizando la fórmula para calcular la muestra $n = \frac{N}{1+\frac{e^2(N-1)}{z^2pq}}$, donde:

Tabla 1. Cálculo de la muestra

Convención	Descripción	Tamaño
n	Número de la muestra	Por calcular
N	Número de la población	40
e	Error muestral o margen de error	.05

Convención	Descripción	Tamaño
z	Nivel de confianza	95% (1.96)
pq	Nivel de varianza de la población	0.25 (para manejar un grado de imparcialidad)

Fuente: Autor del proyecto

Remplazando los valores en la fórmula:

$$n = \frac{40}{1 + \frac{.05^2(40-1)}{(1.96^2)(.25)}}$$

$$n = \frac{40}{1 + \frac{0{,}0975}{0{,}9604}}$$

$$n = \frac{40}{1{,}1015}$$

$$n = 36{,}3134$$

Se realiza aproximación a la unidad arriba, dejando el valor de n en 37.

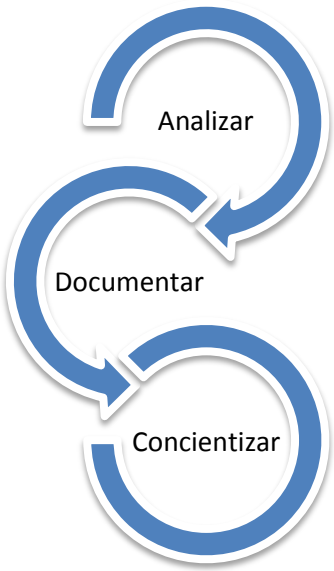
7.4 VARIABLES

a) LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA DE LA CAJA DE PREVISIÓN SOCIAL DE LA UNIVERSIDAD DE CARTAGENA

b) LA O LAS NORMAS CON LAS CUALES VAN A GUIAR EL DESARROLLO DEL PROYECTO

7.5 METODOLOGÍA DE DESARROLLO

Figura 3. Metodología



Fuente: Autor del proyecto

La metodología a aplicar para el presente proyecto es la siguiente:

- Se realizará entrevista con el personal de la oficina de sistemas para establecer los activos con los que cuenta la entidad para el funcionamiento de su sistema de información, así mismo, estableciendo una valoración para cada uno de ellos.

- Se identificarán y valorarán las amenazas para cada activo de acuerdo a la metodología Magerit, para así medir tanto el impacto como el riesgo al que se encuentran expuestos.

- Se realizará inspección visual y entrevistas con los empleados a fin de verificar, en su labor cotidiana, cómo utilizan los equipos informáticos además del sistema de información.

- Se elaborará de acuerdo a la información obtenida, el manual de políticas de seguridad informática.

- Se realizará entrega del manual a la directiva de la entidad para su estudio y aprobación.

- Una vez sea aprobado el manual se procederá a realizar, en conjunto con el Jefe de la División Administrativa o la persona designada, un cronograma de capacitación a los empleados de la Caja de Previsión Social de la Universidad de Cartagena.

- Se realizarán pruebas e inspecciones a fin de verificar el cumplimiento de las políticas de seguridad, y de ser necesario, se sugerirán modificaciones a fin de mejorar el manual.

8. RECURSOS DISPONIBLES

8.1 RECURSOS HUMANOS

Para la realización de este proyecto es necesaria la participación de un (1) ingeniero de sistemas, así como también un (1) digitador que ayudará en la transcripción de entrevistas y tabulación de encuestas que lleguen a realizarse, digitando además toda la información que sea necesaria.

Tabla 2. Recursos humanos

Recurso	Tiempo (horas)	Valor hora	Total
Ingeniero de sistemas	960	$ 15.000	$ 14.400.000
Encuestador/Digitador	200	$ 10.000	$ 2.000.000
Total			**$ 16.400.000**

Fuente: Autor del Proyecto

8.2 RECURSOS FÍSICOS

Es necesario además, la utilización de elementos que faciliten la labor a desempeñar por cada uno de los participantes, siendo los siguientes:

Tabla 3. Recursos Físicos

Recurso	Fuente	Valor
Computador personal	Propios	$ 0
Puesto de trabajo	Entidad	$ 0
Norma ISO 27002	Propios	$ 80.000
Libros	Propios	$ 100.000
Papelería	Propios	$ 100.000
Total		**$ 280.000**

Fuente: Autor del Proyecto

9. CRONOGRAMA

Tabla 4. Cronograma de trabajo

	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO
Describir la situación actual de la empresa						
Realización de entrevistas con el personal de la empresa						
Identificación activos y valoración de amenazas						
Medición de impacto y riesgos						
Desarrollo de políticas de seguridad						
Institucionalización de las políticas						
Capacitación a empleados						
Publicaciones de las políticas						
Realización de pruebas						

Fuente: Autor del Proyecto

10. ANÁLISIS DE RIESGOS

La "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas", conocida por su acrónimo Magerit, surgió debido al crecimiento del uso de las tecnologías de información y comunicaciones (TIC), las cuales generan beneficios para la sociedad. Este método establece los pasos a seguir para gestionar los riesgos que están ligados a cada uno de los activos de la entidad, a fin de garantizar la confianza de los usuarios finales del servicio que presta la Caja de Previsión Social de la Universidad de Cartagena.

10.1 ANÁLISIS DE ACTIVOS

La Caja de Previsión Social de la Universidad de Cartagena cuenta con una locación de diez (10) oficinas administrativas y tres (3) asistenciales, además de cuatro (4) consultorios médicos, un (1) consultorio odontológico, un (1) consultorio fisioterapéutico y una (1) farmacia.

Dentro de las oficinas administrativas, se encuentra la Oficina de Sistemas, en la cual se centra la operación de la entidad. Los activos tecnológicos para la realización del presente análisis son los siguientes:

Tabla 5. Identificación de activos

CÓDIGO	TIPO/CLASE	NOMBRE	DESCRIPCIÓN
ACT1	Información	Bases de datos	Bases de datos de los aplicativos SIAS
ACT2	Software	SIAS	Conjunto de aplicaciones desarrolladas a la medida

CÓDIGO	TIPO/CLASE	NOMBRE	DESCRIPCIÓN
ACT3	Hardware	Puestos de Trabajo	Equipos de trabajo de la entidad. 35 en total
ACT4	Hardware	Servidores	Servidores que soportan las transacciones realizadas en la entidad. 3 en total (Aplicaciones, Proxy, Datos)
ACT5	Red	Router	Permite conexión por wlan en un área determinada
ACT6	Red	Swicth	Switch Dell 48 puertos
ACT7	Red	Patch Panel	Patch panel 48 puertos marca Dell
ACT8	Servicios	ADSL	Servicio ADSL contratado de 4MB con rehuso de 1:6
ACT9	Personal	Empleados	Cada uno de los empleados de la entidad. 40 en total

Fuente: Autor del proyecto

10.2 VALORACIÓN DE LOS ACTIVOS

La metodología Magerit establece cinco (5) dimensiones de seguridad que son:

- Confiabilidad: Propiedad en la que la información no se releva ni se pone a disposición de personas o entes no autorizados.

- Integridad: Propiedad de mantener de sin ninguna alteración la información o un activo.

- Autenticidad: Propiedad consistente en que un ente es quien dice ser, o que se garantiza la fuente de donde provienen los datos.

- Disponibilidad: Que los servicios o activos estén listos para su uso cuando son necesitados.

- Trazabilidad: Se permite verificar qué o quién hizo y cuándo lo hizo.

La valoración de los activos, se realiza de acuerdo a cómo su ausencia o falla afecte cada uno de las dimensiones con una escala de 0 a 10, siendo 0 “Despreciable” y 10 “Daño extremadamente grave”, tal como se muestra en la siguiente tabla:

Tabla 6. Escala de valoración

Valor	**Criterio**	
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: Magerit – versión 3.0 Libro II – Catálogo de Elementos

Una vez identificados los activos y la escala a utilizar, se procede a realizar la valoración de los mismos:

Tabla 7. Valoración de activos

DESCRIPCIÓN			VALORACIÓN				
CÓDIGO	TIPO/CLASE	NOMBRE	Disponibilidad [D]	Integridad [I]	Confidencialidad [C]	Autenticidad [A]	Trazabilidad [T]
ACT1	Información	Bases de datos	9	8	8	8	8
ACT2	Software	SIAS	7	8	9	9	9
ACT3	Hardware	Puestos de Trabajo - 35	5	3	3	4	5
ACT4	Hardware	Servidores - 3	8	7	9	6	9
ACT5	Red	Router	5	3	3	2	1
ACT6	Red	Swicth	9	4	4	5	5
ACT7	Red	Patch Panel	9	4	4	5	5
ACT8	Servicios	ADSL	2	1	1	1	1
ACT9	Personal	Empleados	7	6	7	5	4

Fuente: Autor del proyecto

10.3 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

Magerit contiene una lista extensa de amenazas que afectan a un activo en específico. Una vez determinadas las que se pueden materializar en la Caja de Previsión Social de la Universidad de Cartagena, se procede a darles una valoración usando el sentido de Probabilidad, para lo cual se utilizará la siguiente tabla de frecuencias como patrón a seguir:

Tabla 8. Probabilidad de Frecuencia (FREQ)

Valor	Criterio	
100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada varios años
1/100	Muy poco frecuente	Siglos

Fuente: Magerit – versión 3.0 Libro I – Método

Para cada una de las dimensiones se establecerá un valor en escala porcentual, el cual medirá el impacto que causaría si se llegara a materializar cada una de las amenazas por activos.

Tabla 9. Escala porcentual de impactos

Porcentaje	Criterio
90%-100%	Muy alto
75%-89%	Alto
50%-74%	Medio
20%-49%	Bajo
0%-19%	Muy bajo

Fuente: Autor del proyecto

Tomando una relación entre el impacto y la frecuencia de las amenazas, se establece una matriz con la Escala de Riesgos, en la que se puede apreciar un criterio de qué tan malo puede ser una amenaza para la Caja de Previsión Social de la Universidad de Cartagena. Por ejemplo, un riesgo Muy Frecuente con un impacto Muy Alto, generará un riesgo Muy Alto, mientras que por el contrario si es

Muy poco Frecuente con un impacto Muy Bajo, el riesgo sería Muy Bajo para la entidad.

Tabla 10. Escala de Riesgo

RIESGO		Frecuencia				
		Muy frecuente	Frecuente	Normal	Poco frecuente	Muy poco frecuente
Impacto	Muy alto	MA	MA	A	M	B
	Alto	MA	A	A	M	B
	Medio	A	A	M	B	B
	Bajo	M	M	B	MB	MB
	Muy bajo	B	B	B	MB	MB

Convenciones	
Valor	**Criterio**
MA	Muy alto
A	Alto
M	Medio
B	Bajo
MB	Muy bajo

Fuente: Autor del proyecto

De acuerdo a los criterios de evaluación anteriores, se procede a realizar el análisis de las amenazas para cada uno de los activos de la entidad. Al final de cada amenaza, se obtiene un valor promedio de las dimensiones que son afectadas, tomando este junto con la frecuencia para calcular el nivel de riesgo asociado a la amenaza.

Tabla 11. Análisis de amenazas por activos

AMENAZAS POR ACTIVOS	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
[B] Activos Esenciales								
[ACT1] Bases de datos								
[E.1] Errores de los usuarios	10	10%	10%	10%			10%	B
[E.2] Errores del administrador	1	20%	20%	20%			20%	B
[E.15] Alteración accidental de la información	1		1%				1%	B
[E.18] Destrucción de información	1	1%					1%	B
[E.19] Fugas de información	1			10%			10%	B
[A.5] Suplantación de la identidad del usuario	10		10%	50%	100%		53%	A
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%			20%	M
[A.11] Acceso no autorizado	100		10%	50%			30%	M
[A.15] Modificación deliberada de la información	10		100%				100%	MA
[A.18] Destrucción de información	10	50%					50%	A
[A.19] Revelación de información	10			100%			100%	MA
[IS] Servicios Internos								
[SW] Aplicaciones								
[ACT2] SIAS								
[I.5] Avería de origen físico o lógico	1	50%					50%	M
[E.1] Errores de los usuarios	1	1%	10%	10%			7%	B
[E.2] Errores del administrador	1	20%	20%	20%			20%	B
[E.8] Difusión de software dañino	1	10%	10%	10%			10%	B
[E.15] Alteración accidental de la información	1		1%				1%	B
[E.18] Destrucción de información	1	50%					50%	M
[E.19] Fugas de información	1			10%			10%	B
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%			14%	B
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%				1%	B
[A.5] Suplantación de la identidad del usuario	1		50%	50%	100%		67%	M
[A.6] Abuso de privilegios de acceso	1	1%	10%	10%			7%	B
[A.7] Uso no previsto	1	1%	10%	10%			7%	B
[A.8] Difusión de software dañino	1	100%	100%	100%			100%	A

AMENAZAS POR ACTIVOS	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
[A.11] Acceso no autorizado	1		10%	50%			30%	B
[A.15] Modificación deliberada de la información	1		50%				50%	M
[A.18] Destrucción de información	1	50%					50%	M
[A.19] Revelación de información	1			50%			50%	M
[A.22] Manipulación de programas	1	50%	100%	100%			83%	A
[E] Equipamento								
[HW] Equipos								
[ACT3] Puestos de Trabajo								
[N.1] Fuego	0,1	100%					100%	M
[N.2] Daños por agua	0,1	50%					50%	B
[N.*] Desastres naturales	0,1	100%					100%	M
[I.1] Fuego	0,1	100%					100%	M
[I.2] Daños por agua	0,1	50%					50%	B
[I.*] Desastres industriales	0,1	100%					100%	M
[I.3] Contaminación medioambiental	0,1	50%					50%	B
[I.4] Contaminación electromagnética	1	10%					10%	B
[I.5] Avería de origen físico o lógico	1	50%					50%	M
[I.6] Corte del suministro eléctrico	1	100%					100%	A
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%					100%	A
[1.11] Emanaciones electromagnéticas	1			1%			1%	B
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%			20%	B
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%					10%	B
[E.24] Caída del sistema por agotamiento de recursos	10	50%					50%	A
[E.25] Pérdida de equipos	5	5%		10%			8%	B
[A.6] Abuso de privilegios de acceso	1	10%	10%	50%			23%	B
[A.7] Uso no previsto	1	10%	1%	10%			7%	B
[A.11] Acceso no autorizado	1	10%	10%	50%			23%	B
[A.23] Manipulación del hardware	0,1	50%		50%			50%	B
[A.24] Denegación de servicio	2	100%					100%	MA
[A.25] Robo de equipos	5	5%		10%			8%	B
[A.26] Ataque destructivo	1	100%					100%	A

AMENAZAS POR ACTIVOS	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
[ACT4] Servidores								
[N.1] Fuego	0,1	100%					100%	M
[N.2] Daños por agua	0,1	50%					50%	B
[N.*] Desastres naturales	0,1	100%					100%	M
[I.1] Fuego	0,1	100%					100%	M
[I.2] Daños por agua	0,1	50%					50%	B
[I.*] Desastres industriales	0,1	100%					100%	M
[I.3] Contaminación medioambiental	0,1	50%					50%	B
[I.4] Contaminación electromagnética	1	10%					10%	B
[1.5] Avería de origen físico o lógico	1	50%					50%	M
[1.6] Corte del suministro eléctrico	1	100%					100%	A
[1.7] Condiciones inadecuadas de temperatura o humedad	1	100%					100%	A
[1.11] Emanaciones electromagnéticas	1			1%			1%	B
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%			20%	B
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%					10%	B
[E.24] Caída del sistema por agotamiento de recursos	10	50%					50%	A
[E.25] Pérdida de equipos	1	100%		100%			100%	A
[A.6] Abuso de privilegios de acceso	1	10%	100%	100%			70%	M
[A.7] Uso no previsto	1	10%	10%	100%			40%	B
[A.11] Acceso no autorizado	1	10%	100%	100%			70%	M
[A.23] Manipulación del hardware	0	50%		50%			50%	B
[A.24] Denegación de servicio	2	100%					100%	MA
[A.25] Robo de equipos	0,1	100%		100%			100%	M
[A.26] Ataque destructivo	1	100%					100%	A
[COM] COMUNICACIONES								
[ACT5] Router								
[N.1] Fuego	0,1	100%					100%	M
[N.2] Daños por agua	0,1	50%					50%	B
[N.*] Desastres naturales	0,1	100%					100%	M
[1.1] Fuego	0,1	100%					100%	M
[I.2] Daños por agua	0,1	50%					50%	B
[I.*] Desastres industriales	0,1	100%					100%	M

AMENAZAS POR ACTIVOS	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
[I.3] Contaminación medioambiental	0,1	50%					50%	B
[I.4] Contaminación electromagnética	1	10%					10%	B
[I.5] Avería de origen físico o lógico	1	50%					50%	M
[I.6] Corte del suministro eléctrico	1	100%					100%	A
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%					100%	A
[I.8] Fallo de servicios de comunicaciones	1	50%					50%	M
[1.11] Emanaciones electromagnéticas	1			1%			1%	B
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%			20%	B
[E.9] Errores de [re-]encaminamiento	1			10%			10%	B
[E.10] Errores de secuencia	1		10%				10%	B
[E.15] Alteración de la información	1		1%				1%	B
[E.19] Fugas de información	1			10%			10%	B
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%					10%	B
[E.24] Caída del sistema por agotamiento de recursos	1	50%					50%	M
[E.25] Pérdida de equipos	1	20%		50%			35%	B
[A.5] Suplantación de la identidad	1		10%	50%	100%		53%	M
[A.6] Abuso de privilegios de acceso	1	10%	10%	50%	100%		43%	B
[A.7] Uso no previsto	1	10%	10%	10%			10%	B
[A.9] [Re-]encaminamiento de mensajes	1			10%			10%	B
[A. 10] Alteración de secuencia	1		10%				10%	B
[A.11] Acceso no autorizado	1	10%	10%	50%	100%		43%	B
[A. 12] Análisis de tráfico	1			2%			2%	B
[A. 14] Interceptación de información (escucha)	1			5%			5%	B
[A. 15] Modificación de la información	1		10%				10%	B
[A. 18] Destrucción de la información	1	50%					50%	M
[A. 19] Revelación de información	1			50%			50%	M
[A.23] Manipulación del hardware	0,1	100%		50%			75%	M
[A.24] Denegación de servicio	10	50%					50%	A
[A.25] Robo de equipos	0,1	20%		50%			35%	MB
[A.26] Ataque destructivo	1	100%					100%	A

AMENAZAS POR ACTIVOS	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
[ACT6] Swicth								
[N.1] Fuego	0,1	100%					100%	M
[N.2] Daños por agua	0,1	50%					50%	B
[N.*] Desastres naturales	0,1	100%					100%	M
[1.1] Fuego	0,1	100%					100%	M
[I.2] Daños por agua	0,1	50%					50%	B
[I.*] Desastres industriales	0,1	100%					100%	M
[I.3] Contaminación medioambiental	0,1	50%					50%	B
[I.4] Contaminación electromagnética	1	10%					10%	B
[I.5] Avería de origen físico o lógico	1	50%					50%	M
[I.6] Corte del suministro eléctrico	1	100%					100%	A
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%					100%	A
[I.8] Fallo de servicios de comunicaciones	1	50%					50%	M
[1.11] Emanaciones electromagnéticas	1			1%			1%	B
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%			20%	B
[E.9] Errores de [re-]encaminamiento	1			10%			10%	B
[E.10] Errores de secuencia	1		10%				10%	B
[E.15] Alteración de la información	1		1%				1%	B
[E.19] Fugas de información	1			10%			10%	B
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%					10%	B
[E.24] Caída del sistema por agotamiento de recursos	1	50%					50%	M
[E.25] Pérdida de equipos	1	20%		50%			35%	B
[A.5] Suplantación de la identidad	1		10%	50%	100%		53%	M
[A.6] Abuso de privilegios de acceso	1	10%	10%	50%	100%		43%	B
[A.7] Uso no previsto	1	10%	10%	10%			10%	B
[A.9] [Re-]encaminamiento de mensajes	1			10%			10%	B
[A.10] Alteración de secuencia	1		10%				10%	B
[A.11] Acceso no autorizado	1	10%	10%	50%	100%		43%	B
[A.12] Análisis de tráfico	1			2%			2%	B
[A.14] Interceptación de información (escucha)	1			5%			5%	B

AMENAZAS POR ACTIVOS	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
[A.15] Modificación de la información	1		10%				10%	B
[A.18] Destrucción de la información	1	50%					50%	M
[A.19] Revelación de información	1			50%			50%	M
[A.23] Manipulación del hardware	0,1	100%		50%			75%	M
[A.24] Denegación de servicio	10	50%					50%	A
[A.25] Robo de equipos	0,1	20%		50%			35%	MB
[A.26] Ataque destructivo	1	100%					100%	A
[ACT7] Patch Panel								
[N.1] Fuego	0,1	100%					100%	M
[N.2] Daños por agua	0,1	50%					50%	B
[N.*] Desastres naturales	0,1	100%					100%	M
[1.1] Fuego	0,1	100%					100%	M
[I.2] Daños por agua	0,1	50%					50%	B
[I.*] Desastres industriales	0,1	100%					100%	M
[I.3] Contaminación medioambiental	0,1	50%					50%	B
[I.4] Contaminación electromagnética	1	10%					10%	B
[1.5] Averia de origen físico o lógico	1	50%					50%	M
[1-6] Corte del suministro eléctrico	1	100%					100%	A
[1.7] Condiciones inadecuadas de temperatura o humedad	1	100%					100%	A
[1.11] Emanaciones electromagnéticas	1			1%			1%	B
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%			20%	B
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%					10%	B
[E.24] Caída del sistema por agotamiento de recursos	10	50%					50%	A
[E.25] Pérdida de equipos	1	20%		50%			35%	B
[A.6] Abuso de privilegios de acceso	1	10%	10%	50%			23%	B
[A.7] Uso no previsto	1	10%	1%	10%			7%	B
[A.11] Acceso no autorizado	1	10%	10%	50%			23%	B
[A.23] Manipulación del hardware	0,1	100%		50%			75%	M
[A.24] Denegación de servicio	2	100%					100%	MA
[A.25] Robo de equipos	0,1	20%		50%			35%	MB
[A.26] Ataque destructivo	1	100%					100%	A

AMENAZAS POR ACTIVOS	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
[SS]Servicios subcontratados								
[ACT8] Acceso a Internet								
[1.8] Fallo de servicios de comunicaciones	1	50%					50%	M
[1.9] Interrupción de otros servicios o suministros esenciales	1	50%					50%	M
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%			20%	B
[E.9] Errores de [re-]encaminamiento	1			10%			10%	B
[E.10] Errores de secuencia	1		10%				10%	B
[E.15] Alteración de la información	1		1%				1%	B
[E.18] Destrucción de la información	1	10%					10%	B
[E.19] Fugas de información	1			10%			10%	B
[E.24] Caída del sistema por agotamiento de recursos	1	50%					50%	M
[A.5] Suplantación de la identidad	1		10%	50%	100%		53%	M
[A.6] Abuso de privilegios de acceso	1		10%	50%	100%		53%	M
[A.7] Uso no previsto	1	10%	10%	10%			10%	B
[A.9] [Re-]encaminamiento de mensajes	1			10%			10%	B
[A. 10] Alteración de secuencia	1		10%				10%	B
[A.11] Acceso no autorizado	1		10%	50%	100%		53%	M
[A.12] Análisis de tráfico	1			2%			2%	B
[A.13] Repudio (negación de actuaciones)	1					100%	100%	A
[A.14] Interceptación de información (escucha)	1			5%			5%	B
[A.15] Modificación de la información	1		10%				10%	B
[A.18] Destrucción de la información	1	50%					50%	M
[A.19] Revelación de información	1			50%			50%	M
[A.24] Denegación de servicio	10	50%					50%	A
[P] Personal								
[ACT9] Empleados								
[E.15] Alteración de la información	1		10%				10%	B
[E.18] Destrucción de la información	1	1%					1%	B
[E.19] Fugas de información	1			10%			10%	B
[E.28] Indisponibilidad del personal	1	10%					10%	B

AMENAZAS POR ACTIVOS	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
[A.15] Modificación de la información	1		50%				50%	M
[A.18] Destrucción de la información	1	10%					10%	B
[A.19] Revelación de información	10			20%			20%	M
[A.28] Indisponibilidad del personal	0,1	50%					50%	B
[A.29] Extorsión	0,1	10%	20%	20%			17%	MB
[A.30] Ingeniería social (picaresca)	0,1	10%	20%	20%			17%	MB

Fuente: Autor del proyecto

Una vez que han sido analizadas cada una de las amenazas posibles y su nivel de riesgo, se obtiene la siguiente tabla como resumen, donde se contabiliza el total de amenazas por cada nivel de riesgo:

Tabla 12. Total de amenazas por nivel de riesgos

CRITERIO	TOTAL
Muy alto	5
Alto	27
Medio	59
Bajo	106
Muy bajo	5

Fuente: Autor del proyecto

11. ANÁLISIS DEL DOMINIO POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La norma ISO/IEC 27001:2013 determina que la organización debe establecer una política de seguridad de la información que se amolde al propósito de la organización, incluyendo tanto los objetivos de seguridad cuando estos existen o proporcionando una referencia para el establecimiento de los mismos, así como los compromisos de cumplir con los requisitos relacionados con la norma y el de mejora continua.

Las políticas de seguridad de la información deben estar siempre disponibles y documentadas, además de comunicadas a cada uno de los integrantes de la Caja de Previsión Social de la Universidad de Cartagena

Tabla 13. Análisis del dominio de Política de Seguridad

A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**				
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**				
		Cumple	**No cumple**	**Qué se tiene**	**Recomendaciones a implementar**
A.5.1.1	Políticas para la seguridad de la información		X		Crear un manual de políticas de seguridad informática acorde a los objetivos misionales de la Caja de Previsión Social de la Universidad de

A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**				
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**				
		Cumple	**No cumple**	**Qué se tiene**	**Recomendaciones a implementar**
					Cartagena.
A.5.1.2	Revisión de las políticas para la seguridad de la información		X		Una vez creado el manual de políticas de seguridad, se debe dejar establecido una revisión periódica que permita determinar si las políticas se encuentra funcionando de manera adecuada, así como también la inclusión o remoción de algunas políticas que se consideren necesarias.

Fuente: Autor del proyecto

12. MANUAL DE POLÍTICAS DE SEGURIDAD

12.1 IMPORTANCIA DE LA IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS DE SEGURIDAD

Para la Caja de Previsión Social de la Universidad de Cartagena es necesario realizar la implementación de las políticas de seguridad, ya que son un conjunto de instrucciones y directrices, que sirven como guía para los empleados, donde se establecen criterios de seguridad que deben ser acogidos por cada uno de los integrantes de la organización.

Muchas veces la implementación de unas políticas de seguridad informática falla debido a que se piensa sólo en escribirlas de acuerdo a lo que se cree necesario sin indagar a fondo, o tomando lo que otras entidades han establecido sin saber o entender que cada organización es un mundo distinto con necesidades únicas y como ejemplo de ello se tiene que cada una tiene un organigrama, procesos y procedimientos, normatividad, instalaciones, presupuestos, objetivos de calidad y productividad, etc.; también, es posible que falle debido a que se impone sin escuchar a los demás integrantes del equipo de trabajo, sin asignación de los responsables o sin actividades que permitan que cada empleado las conozca y tenga claro qué es lo que se quiere proteger con ellas. Estas políticas deben estar enmarcadas en los objetivos de la entidad, es decir, son un soporte para el cumplimiento de la misión y la visión que tiene la Caja de Previsión.

Las políticas de seguridad son una gran necesidad que se tiene en la Caja de Previsión Social de la Universidad de Cartagena, ya que una vez implementadas y

en funcionamiento, cada empleado tendrá claro lo que puede hacer al estar dentro de la empresa, protegiendo a la misma de forma general, sabiendo la importancia de la información que depende de cada uno de ellos, aprovechando de la mejor manera los recursos tecnológicos de los cuales se disponen.

Otra forma en que las políticas ayudan en el aumento de la seguridad de la Caja de Previsión Social, es disminuyendo en gran medida el factor del error humano, ya que todos y cada uno de los empleados que laboran en la organización deben ser involucrados tanto en el desarrollo de las mismas así como manteniéndolos capacitados.

El hecho de que siempre se trate de mantener capacitados a los empleados así como tener las políticas correctamente implementadas, corresponden al primer paso para la obtención de una Caja de Previsión Social segura, pero es muy importante que se persista en ellas, así como también las auditorías sobre las mismas, seguir capacitando y realizar, de acuerdo a lo que se establezca, revisiones y actualizaciones para prevenir nuevos ataques, manteniéndose así en un mejor nivel de seguridad.

Por lo anterior, se plantea un documento que se encuentra anexo como Manual de Políticas de Seguridad Informática, que recoge las políticas de seguridad informática necesarias para la entidad, que incluye las siguientes políticas:

- Políticas de Disposición y Manejo de los Equipos de Cómputo
- Políticas de Recursos compartidos
- Políticas de Cuentas de Usuario
- Políticas de Contraseñas de Usuario

- Políticas de Uso de Internet
- Políticas de Correo Electrónico
- Políticas de Administración de Servidores
- Políticas del uso e instalación del software en los equipos de cómputo
- Políticas de Cifrado de información
- Políticas de Seguridad del personal
- Otras Políticas
- Excepciones
- Generalidades
- Sanciones

12.2 LINEAMIENTOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

- Al entregar los datos de una nueva cuenta, el funcionario debe declarar que conoce y aplicará cada una de las políticas y procedimientos establecidos para el uso de la misma, aceptando las responsabilidades por el uso que se le dé a esta.

- Sólo los funcionarios debidamente autorizados, identificados y autentificados, tendrán acceso al sistema operativo y a los sistemas de información, limitados por los roles establecidos de acuerdo a sus funciones y responsabilidades.

- El Área de Sistemas mantiene una separación lógica de las redes para la navegación: acceso a la red institucional e Internet para los trabajadores y acceso internet WIFI para los visitantes.

- El Área de Sistemas estará facultada para filtrar páginas web, de tal modo que se controle el contenido servido y el ancho de banda utilizado. También podrá revisar de forma periódica los logs de navegación.

- La navegación está regida por los principios de control, seguridad y uso racional, controlándose a través de políticas de navegación a través de un proxy.

13. PLAN DE CONCIENTIZACIÓN DE POLÍTICAS DE SEGURIDAD

Una vez que el manual de políticas de seguridad informática resultado de este proyecto para la Caja de Previsión Social de la Universidad de Cartagena, sea aprobado por la Gerencia de dicha entidad, es necesario realizar el plan de divulgación y concientización de las mismas, con el fin de que los trabajadores las conozcan, sepan utilizarlas y de esta forma interioricen conceptos de seguridad informática y buenas prácticas para proteger la información de la entidad.

El propósito general de la concientización del usuario es el de enfocar cada uno de los trabajadores en las políticas de seguridad informática, estableciendo así los comportamientos a reforzar, como por ejemplo: no dejar contraseñas escritas en papeles, elaborar de forma periódica una copia de seguridad, mantener el escritorio limpio, etc., además de esto, darles a entender que la seguridad de los activos informáticos no sólo depende de los especialistas en el tema, sino que cada uno de ellos hacen parte de ello y que son piezas fundamentales en la protección de la información y la Caja de Previsión en general.

Un punto que se debe dejar muy claro en las capacitaciones que se realicen, son los procesos disciplinarios para los usuarios que no tienen sentido de pertenencia hacia la entidad y no cumplen con las políticas. Estos procesos serán diseñados por la alta gerencia.

De igual forma, se recomienda establecer incentivos, ya sean por áreas o de forma personal, premiando de esta forma a los trabajadores que se encuentren comprometidos con el desarrollo y crecimiento de las políticas de seguridad, ya

que así se incentiva y motiva al trabajador, cambiando para bien las costumbres con las que vienen laborando desde hace muchos años.

Al igual que el manual de las políticas de seguridad, la entidad debe aprobar y destinar recursos para el desarrollo del programa de concientización.

Para este plan, se propone realizar las siguientes actividades:

- Definir una mascota de campaña: Así cada vez que sea vista, los empleados recordarán que deben hacer uso de las políticas definidas.

- Pendones o afiches: Ya sean pequeños con algunas políticas importantes para que se mantengan siempre en mente.

- Fondos de pantalla: Establecer un fondo de pantalla predeterminado para cada estación de trabajo, con el fin de que sea visible y accesible para todos.

- Videos o presentaciones: Que contengan imágenes alusivas así como algunas políticas, para que sean presentados en los televisores institucionales o durante reuniones.

- Recordatorios como lapiceros, llaveros, vasos, etc.

- Concursos de preguntas respecto a las políticas de seguridad.

- Folletos para entregar con los desprendibles de pago.

13.1 DISEÑO DE PROPUESTA

13.1.1 Título. Como título para el plan de concientización se propone el siguiente:

La seguridad de la información está en tus manos!

13.1.2 Mascota. La siguiente figura muestra la mascota elegida para la campaña, llevará como nombre Lupe.

Figura 4. Mascota

Fuente: Autor del proyecto

13.1.3 Folletos. Los folletos que se publicarán tanto en los tableros de anuncios, correo electrónico y de forma impresa serán, entre otros, los siguientes:

Figura 5. Folletos

Fuente: Autor del proyecto

Estos folletos pueden ser utilizados también para fondos o protectores de pantalla de los computadores de la entidad.

13.1.4 Videos. Para mantener informados no solo a los empleados sino también a los visitantes y afiliados, es posible utilizar los siguientes videos informativos:

Tabla 14. Videos

TÍTULO	LINK
Conceptos básicos sobre la seguridad de la información	https://www.youtube.com/watch?v=zV2sfyvfqik
La seguridad y su justificación desde el punto de vista del negocio.	https://www.youtube.com/watch?v=6EspTMCxTgM
Definición de las políticas, organización, alcance...	https://www.youtube.com/watch?v=qawa_QcuFfc
Seguridad informática - políticas para cuidar sus datos	https://www.youtube.com/watch?v=jkvpLKRfwt4

Fuente: Autor del proyecto

14. PRUEBAS DE SEGURIDAD DE POLÍTICAS

Para conocer si las personas que laboran en la Caja de Previsión Social de la Universidad de Cartagena se apoderan de las políticas y las ponen en práctica una vez que han pasado por el programa de concientización de las mismas, es necesario realizar algunas pruebas como por ejemplo, una encuesta para medir su nivel de conocimiento. Estas mismas encuestas revelarán si es necesario algún ajuste, ya sea a las políticas, por si ha surgido algún hecho que se haya dejado de lado, o al programa de concientización, por si los empleados desconocen de ellas.

Tabla 15. Pruebas a Políticas de Seguridad Informática a empleados

Caja de Previsión Social de la Universidad de Cartagena				
PRUEBAS A POLITICAS DE SEGURIDAD INFORMÁTICA				
Fecha:	**Hora:**	**Consecutivo:**		
Dependencia:				
Empleado:				
Núm.	**Aspecto a evaluar**	**Si**	**No**	**Observaciones**
1	¿Conoce las funciones que debe desempeñar en su puesto de trabajo?			
2	¿La entidad cuenta con políticas de seguridad informática?			
3	¿Conoce las políticas? (Mencione al menos 2)			
4	¿Ha recibido capacitación respecto a las políticas de seguridad?			
5	¿Maneja o tiene a su cargo activos			

	informáticos? (Mencione cuales son)			
6	¿Tiene acceso a internet desde su computador?			
7	¿Almacena información confidencial en su computador?			
8	¿Comparte esta información por algún medio sin cifrarla?			
9	Realiza periódicamente Copias De Seguridad (Back Up) De La Información (Indicar la periodicidad y dónde la hace)			
10	¿Tiene cuenta de correo electrónico institucional? (Indicar su cuenta)			
11	¿Conoce la clave de acceso a su correo electrónico? (Indicar su clave)			Esta pregunta para verificar si pueden suministrar su clave fácilmente
12	¿Posee clave para acceso al equipo de trabajo?			
13	¿Cambia de forma periódica las claves de acceso al equipo y/o al correo?			

Fuente: Autor del proyecto

Además de esto, se realizaron pruebas a la página web de la entidad en busca de posibles fallos de seguridad como malware en el servidor, así como también un test de penetración y además, se verifica que el proxy esté bloqueando sitios prohibidos en la entidad.

Prueba 1. Verificación online de infecciones o códigos maliciosos en la página web de la entidad.

Esta primera prueba consiste en realizar un escáner a la página web de la entidad, mediante varios sitios que prestan dicho servicio, con el fin de determinar si se encuentran vulnerabilidades que permitan a usuarios maliciosos aprovecharse de éstas y realizar ataques a los afiliados u otras personas que hagan uso de este recurso de la entidad.

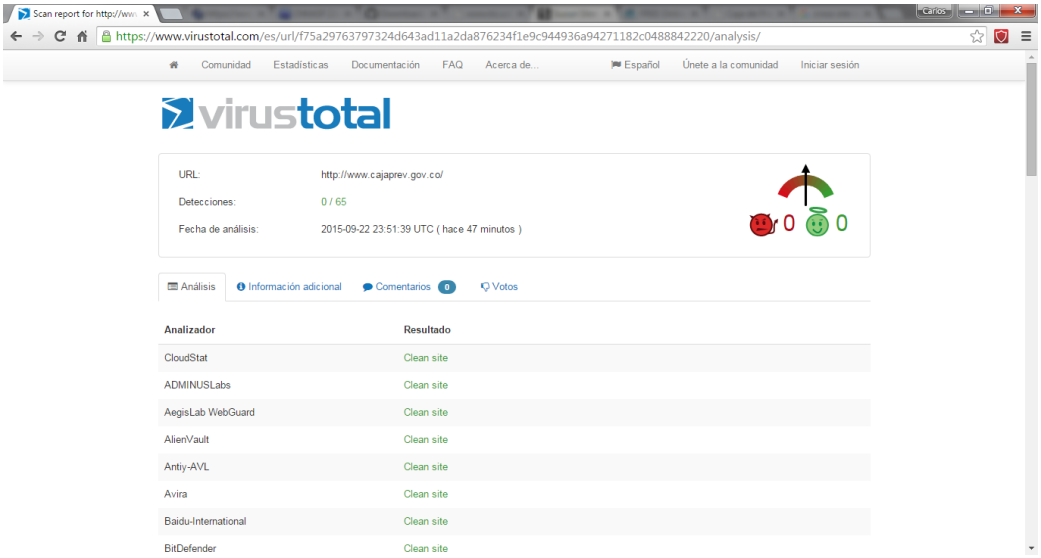
El primer sitio que se utilizará será VirusTotal, disponible en la web: www.virustotal.com. En ella es posible colocar la URL del sitio web a analizar y así obtener un análisis completo del mismo:

Figura 6. Página web de Virus Total

Fuente: http://www.virustotal.com/es

Una vez se termina el análisis, la web muestra un resumen de las pruebas realizadas y las detecciones obtenidas, para el caso en particular, se observa que la página está limpia de virus o infecciones.

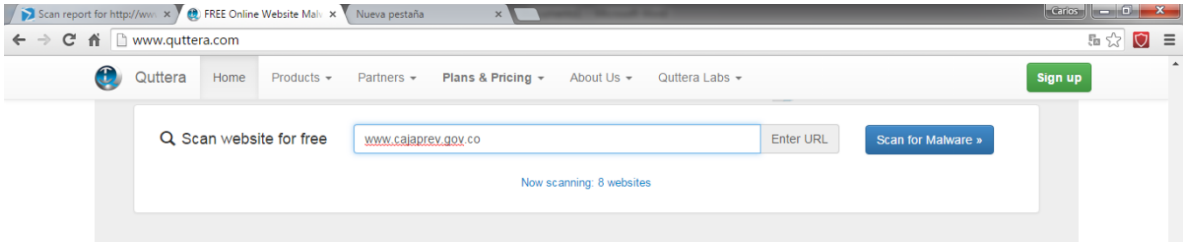
Figura 7. Resultado del escaneo en la web de Virus Total



Fuente: http://www.virustotal.com/es

El segundo sitio es http://www.quttera.com/, siendo la funcionalidad igual al anterior, busca malware en el sitio web:

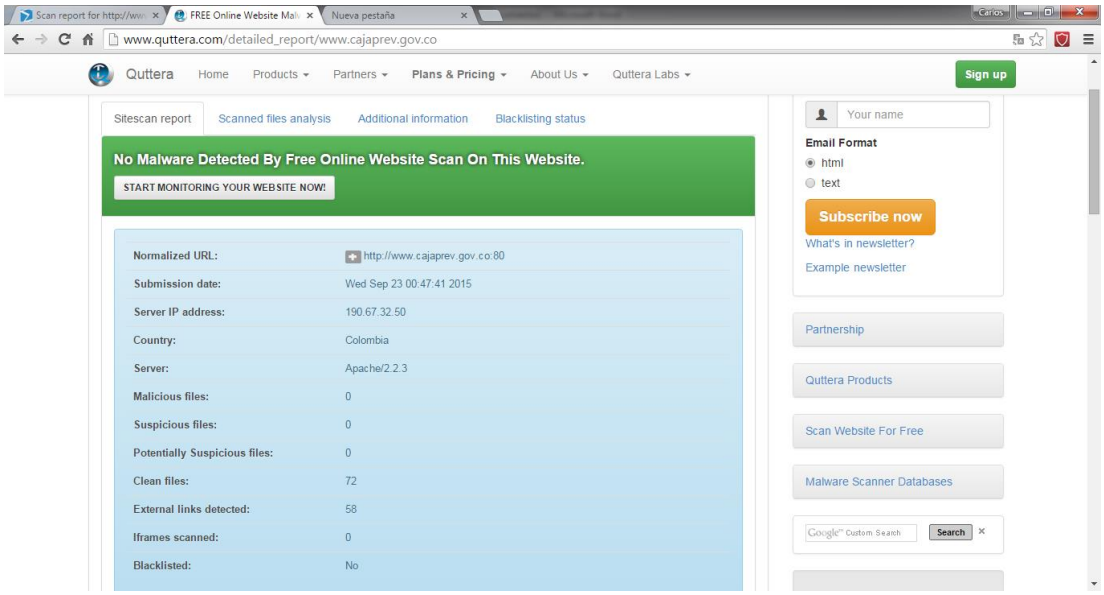
Figura 8. Página web de Quttera



Fuente: http://www.quttera.com/

Este sitio muestra como resultado el siguiente, donde se evidencia que no existe malware:

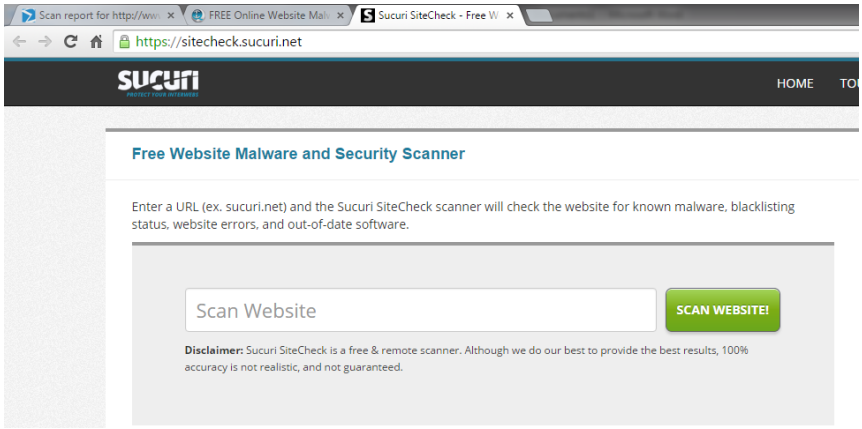
Figura 9. Resultado del escaneo en la web de Quttera



Fuente: http://www.quttera.com/

Y como última web de análisis de malware, se utilizará Sucuri, disponible en https://sitecheck.sucuri.net/

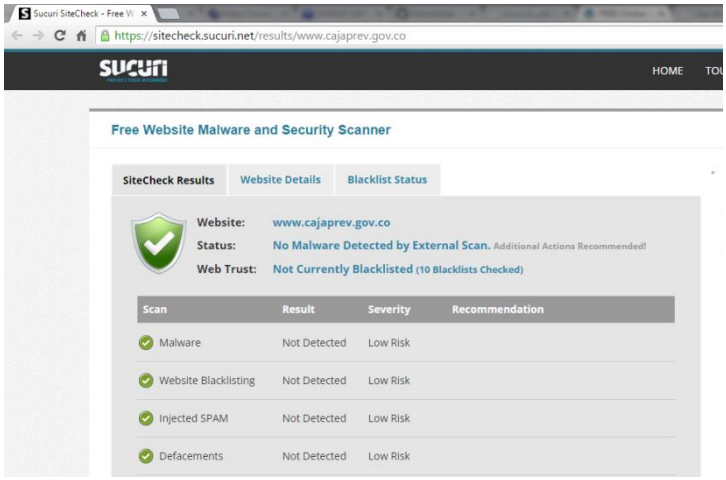
Figura 10. Página web de Sucuri



Fuente: https://sitecheck.sucuri.net/

Siendo los resultados igual a las anteriores, un sitio libre de malware:

Figura 11. Resultado del escaneo en la web de Sucuri

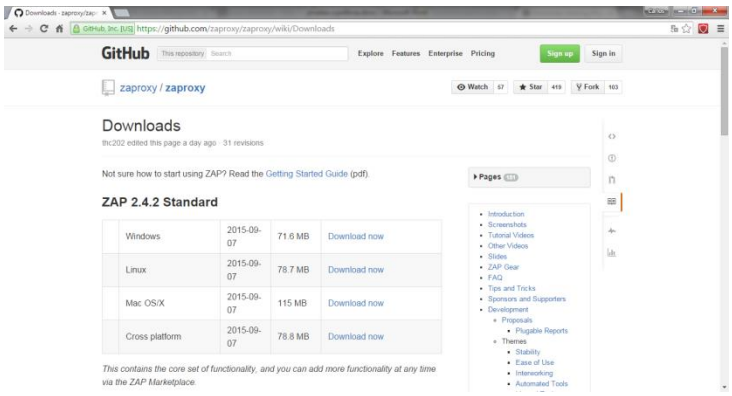


Fuente: https://sitecheck.sucuri.net/

Prueba 2. Verificación con OWASP ZAP.

Para esta prueba, se utiliza el software ZAP 2.4.2 Standard, con la cual se realizará un test completo y automatizado de penetración al sitio web de la entidad, en la que se buscarán vulnerabilidades.

Figura 12. Página de descarga de Zap



Fuente: https://github.com/zaproxy/zaproxy/wiki/Downloads

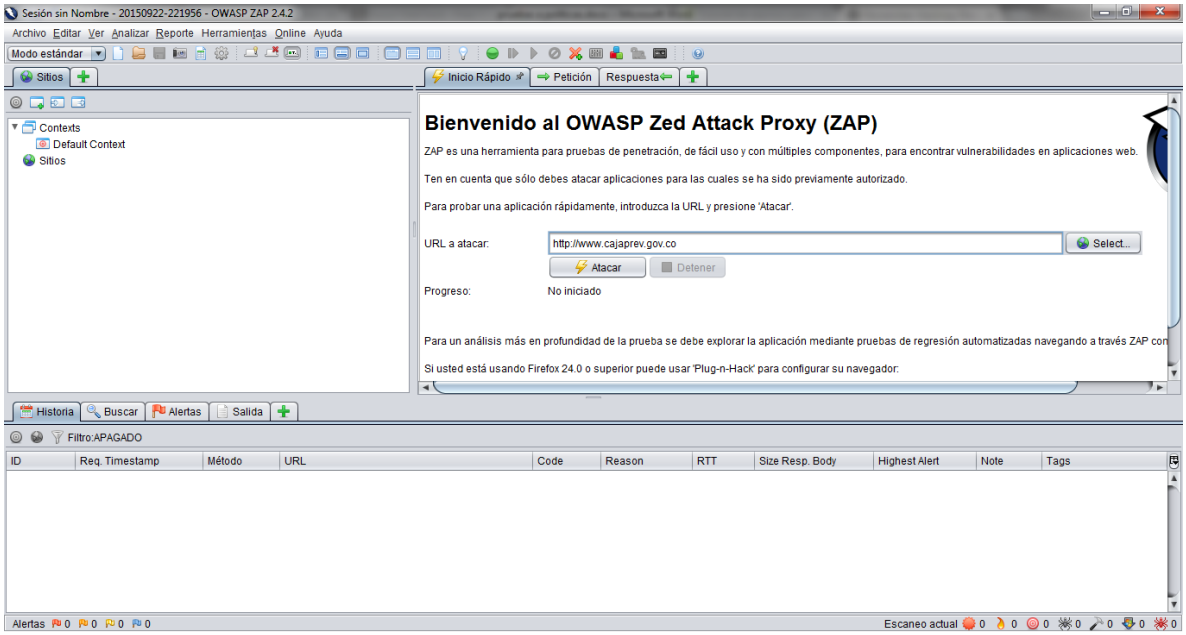
La versión actual es la 2.4.2, la cual se descargará e instalará para la realización del escáner del sitio web.

Figura 13. Ventana de instalación de ZAP

Fuente: Autor del proyecto

Una vez instalado, en la ventana principal del programa hay un campo llamado “Url a atacar”, en la cual se ingresa la web de la Caja de Previsión.

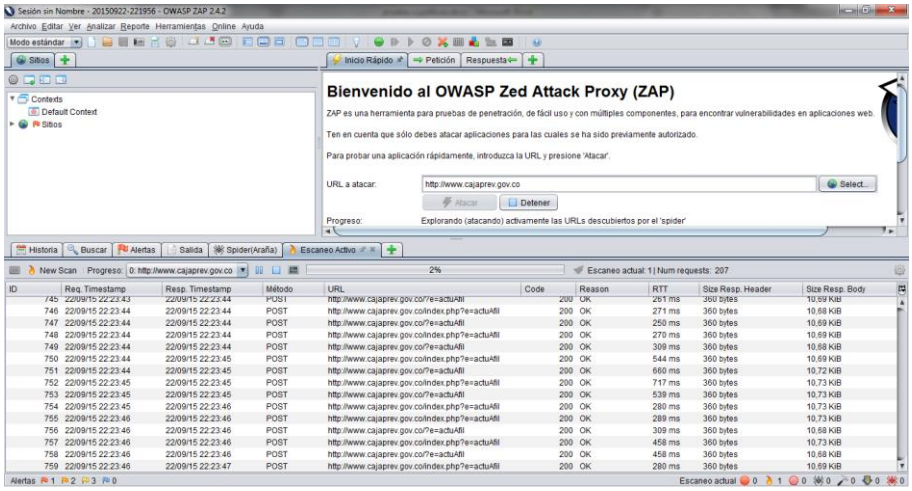
Figura 14. Ventana principal de ZAP



Fuente: Autor del proyecto

Al ingresar la URL del sitio web e iniciar el ataque, el programa empieza por analizar cada una de las entradas del sitio, así como el método de envío de datos (GET o POST)

Figura 15. Ventana de análisis de ZAP

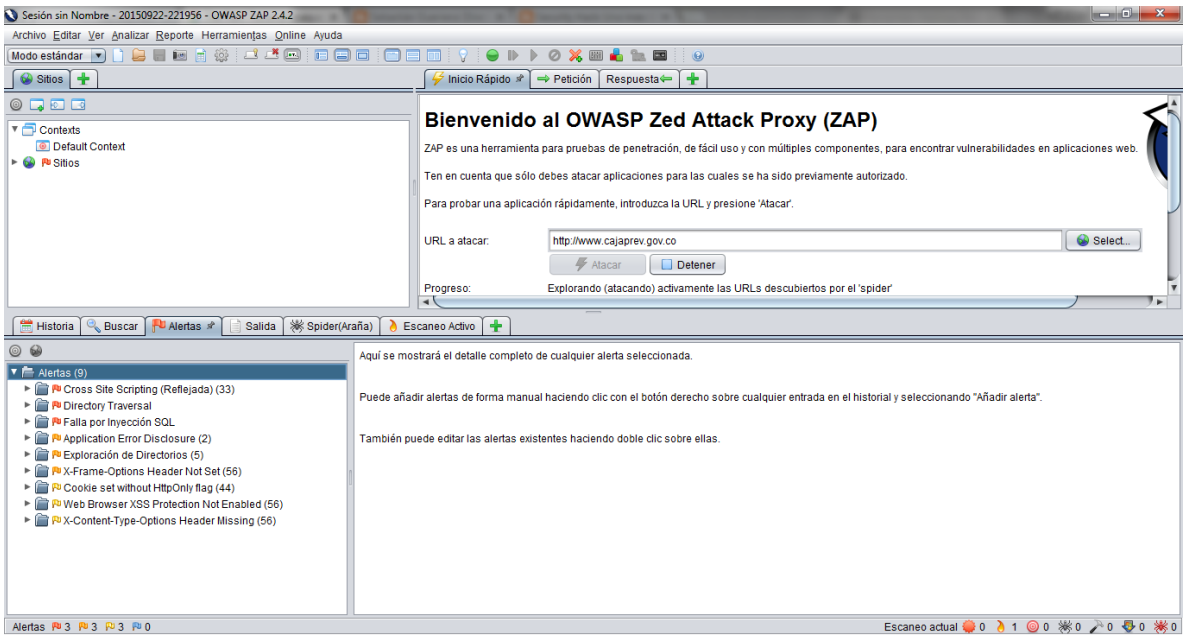


Fuente: Autor del proyecto

Conforme avanza el análisis, se van generando ciertas alertas que son al final, lo que se debe revisar minuciosamente para determinar cuál es el grado de exposición del sitio web y por consiguiente, la red de la entidad.

Al culminar la evaluación del sitio, se evidencia que se generan 9 alertas, entre las cuales se encuentran 3 rojas, queriendo esto decir que deben ser priorizadas con urgencia.

Figura 16. Ventana de alertas de ZAP



Fuente: Autor del proyecto

Como ejemplo, se tomará uno de los formularios dispuestos en la página web de la entidad, que sirve como consulta de los datos de los afiliados a la misma, disponible en el link http://www.cajaprev.gov.co/?e=consultasa y se realizará un simple ataque de Inyección SQL.

Figura 17. Página: Consulta de afiliados

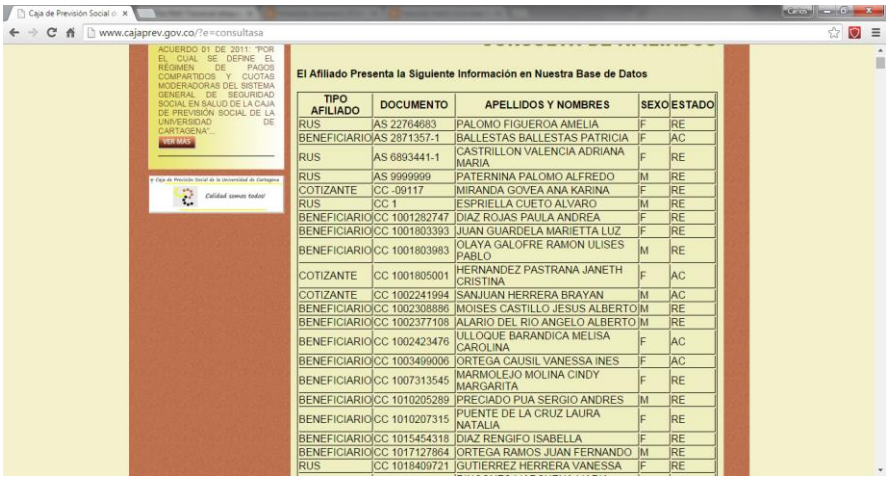
Fuente: www.cajaprev.gov.co/?e=consultasa

Al ingresar en el cuadro de texto para buscar la información de los afiliados de la entidad los caracteres

ZAP' OR '1'='1' --

El formulario devuelve cada uno de los datos contenidos en la tabla de consulta:

Figura 18. Resultado del ataque



TIPO AFILIADO	DOCUMENTO	APELLIDOS Y NOMBRES	SEXO	ESTADO
RUS	AS 22764683	PALOMO FIGUEROA AMELIA	F	RE
BENEFICIARIO	AS 2871357-1	BALLESTAS BALLESTAS PATRICIA	F	AC
RUS	AS 6893441-1	CASTRILLON VALENCIA ADRIANA MARIA	F	RE
RUS	AS 9999999	PATERNINA PALOMO ALFREDO	M	RE
COTIZANTE	CC -09117	MIRANDA GOVEA ANA KARINA	F	RE
RUS	CC 1	ESPRIELLA CUETO ALVARO	M	RE
BENEFICIARIO	CC 1001282747	DIAZ ROJAS PAULA ANDREA	F	RE
BENEFICIARIO	CC 1001803393	JUAN GUARDELA MARIETTA LUZ	F	RE
BENEFICIARIO	CC 1001803983	OLAYA GALOFRE RAMON ULISES PABLO	M	RE
COTIZANTE	CC 1001805001	HERNANDEZ PASTRANA JANETH CRISTINA	F	AC
COTIZANTE	CC 1002241994	SANJUAN HERRERA BRAYAN	M	AC
BENEFICIARIO	CC 1002308886	MOISES CASTILLO JESUS ALBERTO	M	RE
BENEFICIARIO	CC 1002377108	ALARIO DEL RIO ANGELO ALBERTO	M	RE
BENEFICIARIO	CC 1002423476	ULLOQUE BARANDICA MELISA CAROLINA	F	AC
BENEFICIARIO	CC 1003499006	ORTEGA CAUSIL VANESSA INES	F	AC
BENEFICIARIO	CC 1007313545	MARMOLEJO MOLINA CINDY MARGARITA	F	RE
BENEFICIARIO	CC 1010205289	PRECIADO PUA SERGIO ANDRES	M	RE
BENEFICIARIO	CC 1010207315	PUENTE DE LA CRUZ LAURA NATALIA	F	RE
BENEFICIARIO	CC 1015454318	DIAZ RENGIFO ISABELLA	F	RE
BENEFICIARIO	CC 1017127864	ORTEGA RAMOS JUAN FERNANDO	M	RE
RUS	CC 1018409721	GUTIERREZ HERRERA VANESSA	F	RE

Fuente: Autor del proyecto

Para evitar ataques a corto, mediano o largo plazo, se deben tomar medidas correctivas ante este tipo de vulnerabilidades, como son:

- Colocar captchas en los formularios para validar que los intentos son realizados por personas y no por robots o programas automatizados.
- Sólo utilizar el método POST para el envío de datos.
- Limitar la cantidad de datos a ingresar en cada campo de texto (atributo html maxlength)
- Remplazar todos los caracteres especiales que se ingresen en los campos de texto a su forma textual, como por ejemplo el signo &, sería cambiado a &. Al estar el sitio creado en PHP, algunas funciones básicas a utilizar serían htmlspecialchars() y addslashes().
- Las conexiones a las bases de datos deben realizarse con usuarios de perfil limitado.
- Y muy recomendable, antes de subir cualquier formulario a la web, realizarle todas las validaciones posibles para verificar su eficacia ante los ataques.

Prueba 3. Cumplimiento de bloqueo a sitios web prohibidos.

El ingreso a sitios web que no brinden ningún beneficio al trabajador en sus labores diarias, sino que por el contrario sirven de distracción, están siendo bloqueados por el administrador de la red, conforme a las políticas de Uso de Internet en la entidad.

Para esto, fue necesaria la instalación de un Proxy en la red usando el software Squid, para que todas las conexiones pasaran a través de este y así poder filtrar lo

estrictamente permitido. Dos de las páginas bloqueadas son: www.facebook.com y www.youtube.com, debido al alto grado tanto de distracción como de consumo del ancho de banda.

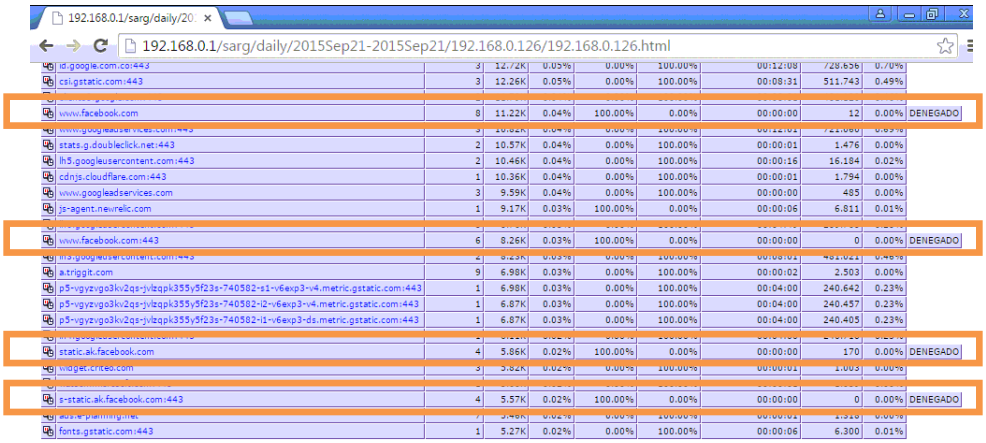
Como herramienta para la generación de reportes de los datos que pasan por el proxy Squid, se instaló el software SARG:

Figura 19. Página inicial de SARG

Fuente: Autor del proyecto

Con SARG, se obtienen diversos reportes, dentro de los cuales se encuentra el acceso a sitios por usuario, y el de sitios bloqueados:

Figura 20. Reporte de conexiones por usuario



Fuente: Autor del proyecto

Como se aprecia, el usuario de ip 192.168.0.126 realizó varios intentos de ingresar a www.facebook.com y a www.youtube.com, páginas web que se encuentran bloqueadas.

Y en el reporte de sitios denegados, se muestran las direcciones IP de los usuarios, así como la fecha y hora del intento de ingreso a uno de los sitios web bloqueados.

Figura 21. Reporte de conexiones bloquedas

Fuente: Autor del proyecto

15. CONCLUSIONES

- Una vez concluido el presente proyecto, la seguridad de la información que posee la Caja de Previsión Social de la Universidad de Cartagena, aumentará de forma notoria al tener elaborado e implementado un manual por cual puedan regirse para contrarrestar los riesgos a los cuales se encuentran expuestos, el cual sirve también como guía para la utilización correcta de los recursos informáticos con los que cuentan los trabajadores de esta entidad de salud.

- Al realizar un análisis de riesgo de la entidad se obtuvo una visión global de la misma, evidenciando que hay falencias en la seguridad informática. Es muy recomendable actualizarlo de manera periódica para mantener al margen nuevas amenazas que puedan surgir de manera futura, ya que los sistemas de información siempre están en constante actualización.

- La elaboración del manual de políticas de seguridad informática tuvo como base la utilización de la norma ISO/IEC 27001:2013, la cual consiste en la creación de un Sistema de Gestión de Seguridad Informática; así como también la norma ISO/IEC 27002:2013 en la que se encuentran las buenas prácticas del manejo de la información, mostrando los dominios y controles para cada uno de ellos, siendo el primero, Política de Seguridad Informática, el aplicado en este proyecto.

- Es muy recomendable que una vez aprobado el documento de Políticas de Seguridad Informática por la Gerencia de la Caja de Previsión Social de la

Universidad de Cartagena, se coloque en marcha su implementación, estableciendo cronogramas de capacitación para sus empleados y mitigar de esta forma los riesgos a los cuales se encuentran expuestos.

- Una vez se realice la implementación, es necesario efectuar pruebas para verificar el cumplimiento de cada una de las políticas utilizando los formatos de encuestas creados en este proyecto y otras que considere la Gerencia o el Área de Sistemas.

- El presente proyecto puede ser tomado como el primer paso para la implementación de un Sistema de Gestión de Seguridad Informática en la entidad, para crear así una mejora contínua en la gestión de la seguridad, garantizando además una continuidad y disponibilidad de las operaciones de la entidad, así como también la reducción de los costos que se deriven por algún incidente informático.

16. RECOMENDACIONES

- Es necesaria la socialización del presente proyecto ante la directiva de la entidad para su aprobación y puesta en marcha.

- La realización de capacitaciones al personal de la Oficina de Sistemas para mejorar sus conocimientos en Seguridad Informática, ayudando de esta forma a promover el tema, difundiendo entre los demás trabajadores la protección de la información que se maneja en la entidad.

- Revisión, evaluación y aprobación del manual de políticas de seguridad informática producto de este proyecto, por parte de la directiva.

- Es completamente necesaria la realización de capacitaciones a cada uno de los trabajadores de la entidad para lograr un alto grado de concientización en los mismos de la importancia de la protección de la información.

- Realizar jornadas de simulacros de un desastre informático una vez sean implementadas y aprobadas las políticas de seguridad, para medir a profundidad los beneficios logrados.

- Las políticas de seguridad informática, son el primer paso para la implementación de un Sistema de Gestión de Seguridad Informática (SGSI), por lo que se espera que se adopten las medidas necesarias, así como también se destinen recursos para la implementación de un SGSI y cumplir a cabalidad con lo establecido en la norma ISO/IEC 27001:2013.

BIBLIOGRAFÍA

BORGHELLO, Cristian. Segu.Info. Políticas de Seguridad de la Información. [En línea]. <http://www.segu-info.com.ar/politicas/polseginf.htm>. [Citado en 4 de Diciembre de 2014].

COLOMBIA. MINISTERIO SALUD Y LA PROTECCIÓN SOCIAL. Resolución 1995 de 1999 (8, Julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clínica. Bogotá: El Ministerio, 1999. 8 p.

CASTAÑO GALVIS, Wilson y GONZÁLEZ SANABRIA, Yina Alexandra Fundamentos de seguridad de la informacion. Bucaramanga: Universidad Nacional Abierta Y A Distancia UNAD, 2012.

CRISTIANSE, Eric. Concientización en Seguridad de la Información. [En línea]. <http://www.cybsec.com/upload/Molinos_Jornada_Cybsec_Eric_Cristianse.pdf> [Citado en 10 de Mayo de 2015].

GUÍA DE SEGURIDAD DE LAS TIC [En línea]. <https://www.ccn-cert.cni.es/publico/herramientas/pilar44/en/help/manual_usuario_pilar_basic-4.3.pdf> [Citado en 17 de Abril de 2015].

LOBO PARRA, Leonard David y OVALLOS OVALLOS, Jesús Andrés y SIERRA GÓMEZ, Ana María. Plan de gestión de la seguridad de la información de la Biblioteca Argemiro Bayona de la Universidad Francisco de Paula Santander Ocaña, mediante la aplicación de la norma ISO 27001 y técnicas de ethical hacking. Ocaña, 2012, 33 h. Trabajo de grado (Especialista en Auditoría De Sistemas). Universidad Francisco De Paula Santander Ocaña, Facultad de Ingeniería. Disponible en:

<http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/325/1/25095.pdf>

MAGERIT Seguridad Informatica. [En línea]. <http://seguridadinformaticaufps.wikispaces.com/MAGERIT> [Citado en 19 de Abril de 2015].

MAGERIT – versión 3.0 Libro I - Método [En línea]. <http://administracionelectronica.gob.es/ctt/resources/7e6c82fb-9607-43e3-a70b-080a27a02bf7?idIniciativa=184&idElemento=85> [Citado en 17 de Abril de 2015].

MAGERIT – versión 3.0 Libro II - Catálogo de Elementos [En línea]. <http://administracionelectronica.gob.es/ctt/resources/a9fff834-15f6-499b-ae5f-ff7b9989ddc5?idIniciativa=184&idElemento=86> [Citado en 17 de Abril de 2015].

MAGERIT – versión 3.0 Libro III - Guía de Técnicas [En línea]. <http://administracionelectronica.gob.es/ctt/resources/01e54e9c-bf49-4b85-aa40-e3dccbcb13d3?idIniciativa=184&idElemento=87> [Citado en 17 de Abril de 2015].

MIFSUD, Elvira. Monográfico: Introducción a la seguridad informática - Políticas de seguridad. En: Observatorio Tecnológico del Gobierno de España. [En línea]. <http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=4> [Citado en 3 de Diciembre de 2014].

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMBA, Mildred. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Popayán, 2014, 132 h. Trabajo de grado (Especialista en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD, Escuela

de Ciencias Básicas Tecnología e Ingeniería. Disponible en: <http://repository.unad.edu.co/bitstream/10596/2655/3/76327474.pdf>.

PILAR EAR / [En línea]. <http://www.pilar-tools.com/es/tools/pilar/v53/help_es/cia/index.html> [Citado en 18 de Abril de 2015].

ROMO VILLAFUERTE, Daniel y VALEREZA CONSTANTE, Joffre. Análisis e implementación de la norma ISO 27002 para el departamento de Sistemas de la Universidad Politécnica Salesiana sede Guayaquil. Guayaquil, Ecuador, 2012, 183 h. Trabajo de grado (Ingeniero en Sistemas con mención en Telemática). Universidad Politécnica Salesiana, Facultad de Ingeniería. Disponible en: <http://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf>.

SABOGAL ROZO, Esther Angélica. Proyecto De Seguridad Informática I. La Plata: Universidad Nacional Abierta y a Distancia UNAD, 2013.

SÁNCHEZ SÁNCHEZ, Esteban. Análisis y gestión de riesgos en la UPCT con PILAR [En línea]. <http://www.rediris.es/difusion/eventos/foros-seguridad/fs2012/archivo/analisis_riesgos_upct.pdf> [Citado en 17 de Abril de 2015] .

SECURITY ART WORK. Análisis de riesgos con PILAR (II). [En línea]. <http://www.securityartwork.es/2012/11/13/analisis-de-riesgos-con-pilar-ii/> [Citado en 18 de Abril de 2015].

SUÁREZ SIERRA, Lorena. Sistema de Gestión de la Seguridad de la Información. Bogotá : Universidad Nacional Abierta y a Distancia UNAD, 2013.

UNIVERSIDAD NACIONAL DE COLOMBIA. Guía para elaboración de políticas de seguridad. [En línea]. <http://www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf> [Citado en 11 de Abril de 2015].

VILLAMIZAR R, Carlos. Jugando a crear cultura de seguridad de la información – De la teoría a la práctica. [En línea]. <http://www.magazcitum.com.mx/?p=2361#.VXHGhM9_Oko> [Citado en 10 de Mayo de 2015].

ANEXOS

ANEXO A. Formato Reporte de Incidente

Caja de Previsión Social de la Universidad de Cartagena		
FORMATO REPORTE DE INCIDENTE		
Datos del Reporte		
Fecha:	**Hora:**	**Consecutivo:**
Datos del incidente		
Fecha:	**Hora:**	
Dependencia:		
Descripción del incidente:		

Quien reporta	**Quien recibe el reporte**
Nombre	**Nombre**
Firma	**Firma**

ANEXO B. FORMATO CREACIÓN/MODIFICACIÓN DE USUARIOS

Caja de Previsión Social de la Universidad de Cartagena

FORMATO CREACIÓN/MODIFICACIÓN DE USUARIOS

Fecha:	**Hora:**	**Consecutivo:**
Dependencia:		
Responsable:		

Solicitud	**Nombre**	**Cédula**	**Área**	**Cargo**	**Observa-ciones**

Tipo de Solicitud		**Jefe División Administrativa**
C	**Creación de Usuario**	**Nombre**
R	**Reactivación**	
M	**Modificación**	**Firma**
E	**Eliminación**	

Jefe de Área	**Jefe de Sistemas**
Nombre	**Nombre**
Firma	**Firma**

ANEXO C. MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

CAJA DE PREVISIÓN SOCIAL DE LA UNIVERSIDAD DE CARTAGENA

MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

MAYO DE 2015

INFORMACIÓN DEL DOCUMENTO

Versión	Fecha	Elaborado por	Razón de la actualización
1	05/05/2015	Ing. Carlos Lara Orozco	Creación del documento

CONTENIDO

POLÍTICAS DE SEGURIDAD INFORMATICA DE LA CAJA DE PREVISIÓN SOCIAL DE LA UNIVERSIDAD DE CARTAGENA

INTRODUCCIÓN

Con el aumento de la necesidad de la utilización de las tecnologías de información, entre ellas el uso de equipos de cómputo y los sistemas operativos para su funcionamiento, se hace necesario mantener dentro de los límites de control para el manejo de dichos dispositivos, maximizando las ventajas y evitando el uso indebido para minimizar los problemas que puedan presentarse en los bienes y servicios de la Caja de Previsión Social de la Universidad de Cartagena.

El presente documento sirve de instrumento para cada uno de los funcionarios de la entidad, dando lineamientos de estricto cumplimiento, concientizándolos sobre el correcto uso de los equipos, sistemas operativos y sistemas de información, la sensibilidad de los datos manejados por los mismos así como sus debilidades y fallas, para que sean superadas en caso de presentarse.

ALCANCE

Las políticas que aquí se documentan, son de implementación obligatoria para todos los funcionarios de la Caja de Previsión Social de la Universidad de Cartagena, que hagan uso directa o indirectamente de tecnologías de información y comunicaciones.

COMPROMISO DE LA DIRECCIÓN

Como una muestra del compromiso que la Gerencia de la Caja de Previsión Social de la Universidad de Cartagena con el diseño e implementación de las políticas de seguridad informática en la entidad, aprueba las políticas contenidas en este documento, así como también su apoyo en:

- El fomento de manera activa para la creación de una cultura de seguridad dentro de la entidad.
- Divulgación de estas políticas a cada uno de los funcionarios de la entidad.

- Verificación de que las políticas del presente manual se cumplan a cabalidad.

ACTUALIZACIÓN

Por las consideraciones establecidas en este documento, se revisará por lo menos una vez cada seis (6) meses para actualizarlo y/o agregar nuevas políticas que permitan el adecuado uso de las tecnologías de información y los sistemas operativos en la Caja de Previsión Social de la Universidad de Cartagena.

LINEAMIENTOS DE POLÍTICAS

Toda información que se utilice en los equipos de cómputo y por supuesto, bajo el uso de los sistemas operativos y de información de la Caja de Previsión Social de la Universidad de Cartagena, será de carácter confidencial, por lo que ningún funcionario podrá hacer uso de ella con fines personales, tampoco podrá facilitarla a personal externo en cualquier forma de transmisión.

Los equipos designados a cada funcionario serán de su uso exclusivo y con fines laborales, siendo responsable de los daños realizados al mismo o al sistema operativo. Será un agravante si el uso indebido se realiza con fines lucrativos.

POLÍTICAS DE SEGURIDAD

PSI-CPS-001. Disposición y Manejo de los Equipos de Cómputo

De ser necesario, se asignará a cada funcionario una estación de trabajo para apoyar al cumplimiento de sus labores.

- Estos equipos son parte del patrimonio de la entidad.
- Cada usuario es responsable del equipo que se le asigne o facilite, por lo que debe procurar su cuidado.
- No se permite el traslado de los equipos de cómputo o sus partes a un área distinta a la que fue asignado. Para poder realizarlo se debe solicitar por escrito al Jefe del Área de Sistemas.

- Solo el personal del Área de Sistemas está facultado para abrir, desarmar, cambiar o instalar piezas del equipo de cómputo, así como formatear, instalar, reinstalar o modificar el sistema operativo o cualquier otro programa en la estación de trabajo.
- No es permitido el uso de dispositivos de almacenamiento extraíbles como memorias USB o discos externos.
- Los equipos deben estar conectados correctamente en los tomas de corriente regulada.
- Evitar la exposición directa al sol o al polvo.
- No está permitido fumar así como tampoco el consumo de alimentos y/o bebidas en los puestos de trabajo.
- Informar de forma oportuna cualquier incidente que impida el buen funcionamiento del equipo y/o del sistema operativo al Área de Sistemas (Formato Reporte de Incidente).
- Las solicitudes de instalación o cambio, ya sea del equipo completo o alguna de sus partes, deben ser aprobadas por los jefes del área solicitante y del Área de Sistemas.

PSI-CPS-002. Recursos compartidos

La institución asignará a cada usuario una cuenta para el ingreso a la red de datos, con la cual podrán acceder a una carpeta personal así como otra para compartir archivos con los demás usuarios. Para el correcto uso y funcionamiento, se establecen las siguientes políticas:

- Deben ser utilizados solo por personal de la entidad.
- Los directorios asignados deben utilizarse sólo para fines institucionales, evitando guardar archivos personales además de fotos, música, videos o material innecesario.
- Realizar una copia de seguridad de la información vital para el área de trabajo, al menos una vez al mes por cada usuario (Máximo 50MB por usuario).

- Evitar acceder, modificar o borrar información privada de otros usuarios ajenos a su propiedad.

- Los archivos y carpetas almacenados en la red son propiedad de la entidad, sin que exista un derecho particular sobre ellos.

PSI-CPS-003. Cuentas de Usuario

Cada funcionario debe estar identificado para acceder al sistema operativo y al sistema de información mediante una cuenta de usuario, la cual tendrá ciertos permisos o privilegios dependiendo del rol asignado. Para este ítem se aplicarán las siguientes políticas:

- Toda solicitud de creación de cuenta o modificación de la misma debe realizarse por escrito (Jefe del Área Administrativa o quien realice las funciones de Gestión Humana), debidamente autorizada por los jefes del área solicitante y del Área de Sistemas (Formato Creación/Modificación de usuarios).

- Sólo el Jefe del Área de Sistemas podrá eliminar una cuenta de usuario.

- El Jefe del Área Administrativa o quien realice las funciones de Gestión Humana, deberá informar de manera oportuna situaciones que impliquen creación, modificación y/o borrado de cuentas de usuario, tales como rotación de personal, despidos o renuncias, etc., con el fin de mantener la base de datos de usuarios actualizada (Formato Creación/Modificación de usuarios).

- No se crearán cuentas de Invitado, tampoco a personal externo.

PSI-CPS-004. Contraseñas de Usuario

Se verifica que el usuario que intenta ingresar al sistema sea quien dice ser, mediante un mecanismo de autenticación, compuesto por la combinación de usuario y contraseña.

- La contraseña es un conjunto de caracteres que cada funcionario debe entregar al sistema operativo y a la aplicación de la entidad para poder hacer uso del equipo, debe contener caracteres en minúsculas y mayúsculas, números y al menos un carácter especial, completando un

mínimo de ocho (8) caracteres, siendo así robusta y difícil adivinar por terceros.

- El usuario y la contraseña deben ser de uso personal, siendo el dueño responsable de todas las acciones realizadas.
- Se debe mantener de forma confidencial, ya que sólo el dueño debe conocerla.
- Queda prohibido imprimir, escribir o mostrar la combinación de usuario y contraseña.
- Se limitará a 3 intentos de acceso, después de éstos, se suspenderá por quince (15) minutos la cuenta. Si es necesaria la activación en menor tiempo, debe ser solicitado por escrito (Formato Creación/Modificación de usuarios: Solicitud R - Reactivación), debidamente autorizada por los jefes del área solicitante y del Área de Sistemas.

PSI-CPS-005. Uso de Internet

La Caja de Previsión Social de la Universidad de Cartagena permitirá el acceso a internet a sus funcionarios, de acuerdo a las siguientes políticas:

- Se utilizará solamente para fines laborales, evitando de esta forma saturar el ancho de banda, haciendo buen uso del servicio.
- Queda prohibido el ingreso a redes sociales, páginas de entretenimiento, pornografía, violencia o cualquier otra ajena a las funciones diarias.
- Queda prohibida la descarga de material ilícito o de contenido con derechos de autor.
- No está permitida instalación de software que utilice el ancho de banda para acceder o descargar cualquier contenido, o para realizar llamadas nacionales o internacionales.

PSI-CPS-006. Correo Electrónico

Es una herramienta que facilitará la comunicación del dueño de la cuenta, apoyando la gestión institucional de la empresa.

- Sólo se permitirán usuarios permanentes de la institución.
- Toda comunicación debe ser de carácter laboral.
- Queda prohibido iniciar o responder cadenas de correo electrónico de cualquier tipo.
- Los usuarios deben ser precavidos al abrir mensajes de personas desconocidas, evitando abrir archivos adjuntos que puedan afectar el software instalado en el equipo.
- Evitar el envío de correos de forma masiva, enviando los mensajes sólo a personas estrictamente necesarias.
- Se limita el tamaño de envío y recepción de mensajes a 5MB de información adjunta.
- No facilitar el usuario y la contraseña a terceras personas.
- Queda prohibido el envío de correos con material ilícito, contenido sexual o violento.

PSI-CPS-007. Administración de Servidores

En relación a los servidores y el Área de Sistemas, se establecen las siguientes políticas:

- El área de los servidores, debe permanecer con acceso restringido, sólo el personal autorizado tiene permitido el ingreso.
- Cualquier persona externa que ingrese a la Oficina de Sistemas, debe registrarse en la bitácora de ingreso, proporcionando su nombre, firma y motivo de ingreso.
- Queda prohibida la manipulación de los equipos del área de servidores por personal no autorizado para ello.
- Un conjunto de copias de seguridad de la información de los servidores debe ser trasladada a otros sitios seguros.
- Todos los equipos deben estar conectados a un sistema de alimentación ininterrumpida de corriente eléctrica.

- El cuarto de servidores debe estar en la temperatura adecuada, manteniendo un segundo aire acondicionado de respaldo.

PSI-CPS-008. Del uso e instalación del software en los equipos de cómputo

- El Área de Sistemas será la encargada de determinar de acuerdo con las necesidades particulares de los funcionarios cual es el software a instalar en los equipos de cómputo.
- Solo el Área de Sistemas puede realizar instalaciones, modificaciones de software y de las configuraciones del mismo en los equipos de cómputo.
- Solo se tendrá instalado software que este licenciado y que sea de carácter legal.
- Se podrá instalar software tipo Free, GNU, Shareware, Demos partiendo de un análisis de licenciamiento, seguridad, y de una necesidad particular solicitada expresamente por el usuario o cualquier persona autorizada mediante carta dirigida al jefe del Área de Sistemas y que lo considere necesario para el desarrollo de sus funciones administrativas.

PSI-CPS-009. Cifrado de Información

La Caja de Previsión Social de la Universidad de Cartagena, deberá mantener cifrada la información reservada o restringida durante su almacenamiento y/o transmisión por cualquier medio con el fin de mantener la confiabilidad e integridad de la misma.

- El Área de Sistemas debe establecer un procedimiento para la verificación que los programas o aplicativos que requieran la transmisión de información clasificada como reservada o restringida cuenten con algún método adecuado de cifrado de datos.
- Durante el desarrollo de aplicaciones propias o en la contratación con terceros para este fin, se debe asegurar que los sistemas construidos cumplan con el cifrado de la información establecido en la entidad.

PSI-CPS-0010. Seguridad del Personal

El factor humano es muy importante en el mantenimiento de la seguridad de la información de la entidad, por lo que se debe contar con el personal mejor calificado para cada uno de los cargos.

- El Jefe de la División Administrativa o quien realice las funciones de Gestión Humana, debe asegurar antes de la realización de una contratación las responsabilidades de seguridad, describiendo de forma clara y precisa el cargo, así como los términos y condiciones del contrato, el cual debe incluir una cláusula de confiabilidad y cumplimiento de las políticas de seguridad del presente documento.
- El Jefe de la División Administrativa o quien realice las funciones de Gestión Humana, debe validar que la información suministrada por los aspirantes a algún cargo disponible sea verás, antes de que su vinculación definitiva.
- El Jefe de la División Administrativa o quien realice las funciones de Gestión Humana, debe desarrollar un programa de concientización sobre protección de la información para todo el personal.
- Todo el personal deberá asistir a los cursos que se impartan dentro del programa de concientización, aplicando los conocimientos adquiridos en sus puestos de trabajo.
- Cuando se dé por finalizado un contrato, el personal saliente debe firmar un acuerdo de confidencialidad para evitar la fuga de información sensible o clasificada como reservada.

PSI-CPS-0011. Otras Políticas

Existen algunas políticas de seguridad que no están establecidas en los apartados anteriores; por lo que se establecerán a continuación:

- No se brindará soporte técnico a equipos personales de los funcionarios ni cualquier otra persona, debido a que no son propiedad de la entidad.
- No deben ser cambiadas ninguna de las configuraciones del sistema operativo, como por ejemplo, las direcciones IPs.
- No utilizar el espacio en disco de los equipos con archivos que no sean necesarios para el desarrollo de sus funciones.
- Todos los funcionarios deben apagar completamente los equipos al finalizar su jornada laboral con el fin de ahorrar energía eléctrica.

PSI-CPS-0012. Excepciones

Existirán algunos casos en los que no aplica una política específica, ya que no pueden ser creadas e impuestas en un 100% para todas las actividades de la institución. En los casos en que sea necesaria la ejecución de acciones que estén en conflicto con una o varias políticas estipuladas en este documento, se procederá de acuerdo a la siguiente instrucción:

- Cualquier funcionario que siguiendo sus obligaciones laborales observe la necesidad de aplicarse una excepción a una determinada política, deberá informarla por escrito al Área de Sistemas, el cual evaluará el caso y determinará si es o no válida la excepción, basándose en un análisis de riesgos. En caso de ser válida, enviará comunicación por escrito informando la duración de la excepción y los riesgos a los cuales se expondrá, informando los pasos que debe seguir. Al finalizar el tiempo expuesto, se valorará la continuidad de la excepción, que deberá ser evaluada y aprobada nuevamente, siguiendo los mismos lineamientos.

PSI-CPS-0013. Generalidades

Todo personal de la entidad, está obligado a reportar cualquier vulnerabilidad, riesgo o inconveniente presentado, con el fin de evaluarlos y seguir ajustando el presente documento y los planes de contingencia dispuestos para los equipos de cómputo y el sistema operativo en cada uno de ellos. Por lo anterior, el personal del Área de Sistemas debe mantener un sentido ético y responsable de la información recibida de carácter personal y/o confidencial.

PSI-CPS-0014. Sanciones

Todo el personal de la entidad queda sujeto al cumplimiento de las normas aquí expuestas, so pena de ser sancionado disciplinaria y/o legalmente, si hubiera lugar a ellas. Las sanciones van desde un llamado de atención hasta la suspensión del cargo, dependiendo de la gravedad de la falta cometida, además de la malicia o perversidad con que se cometa.

La Ley 1273 establece los atentados contra los sistemas de información, afectando la confidencialidad, integridad y disponibilidad de los datos, para lo cual se regirá de acuerdo a ésta o las leyes que la modifiquen para efectos de sanciones legales.