FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

"Análisis de Riesgos de los activos de información de la Clínica Internacional – Piura aplicando la metodología MAGERIT"

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERA DE SISTEMAS

AUTORA:

VALDIVIEZO MOGOLLÓN, YESENIA STEPHANIE

ASESORA:

ING. QUITO RODRÍGUEZ, CARMEN ZULEMA

LÍNEA DE INVESTIGACIÓN:

AUDITORIA DE SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN

PIURA – PERÚ

2016

PÁGINA DEL JURADO

ING. JAIME LEANDRO MADRID CASARIEGO
PRESIDENTE

ING. ADÍN SAÚL VELASCO CAMPOVERDE
SECRETARIO

MG. MÁXINO JAVIER ZEVALLOS VÍLCHEZ

VOCAL

DEDICATORIA

A mi padre, por el empeño y trabajo durante estos años, para que pueda lograr mis metas y mis objetivos. A mi madre, por el apoyo incondicional y la confianza puesta en mí hasta el día de hoy y la motivación brindada a lo largo de mi carrera profesional

AGRADECIMIENTO

En primer lugar agradecer a mi familia por el apoyo y la confianza brindada.

Agradecer a la Clínica Internacional - Piura, al personal del área de informática, y a todas aquellas personas que me brindaron su espacio, tiempo y apoyo para el desarrollo de esta investigación.

Agradecer también al asesor metodólogo al Mg. Vélez Ubillús, Luis Felipe y a la Ing. Quito Rodríguez, Carmen Zulema y los diferentes docentes quienes me han apoyado para poder culminar esta investigación.

DECLARACION DE AUTENCIDAD

Yo, Yesenia Stephanie Valdiviezo Mogollón estudiante de la escuela profesional de Ingeniería de Sistemas de la Universidad César Vallejo, filial Piura; declaro que el trabajo académico titulado “Análisis de Riesgos de los activos de información de la Clínica Internacional – Piura aplicando la metodología MAGERIT” presentada, en 212 folios para la obtención del título profesional de Ingeniería de Sistemas es de mi autoría.

Por tanto, declaro lo siguiente:

- He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajos académicos.
- Ni he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.
- Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro título profesional.
- Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.
- De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinan el procedimiento disciplinario.

Piura, 08 de Julio del 2016

_____

Yesenia Stephanie Valdiviezo Mogollón

DNI N°: 46764883

PRESENTACIÓN

En el presente proyecto denominado “Análisis de riesgos de los activos de información de la Clínica Internacional – Piura aplicando la metodología MAGERIT”, se pretende conocer el estado actual en relación a los riesgos de los activos de información que la organización en estudio posee, aplicando una de la metodología más utilizada, por la estructuración de sus tareas y conjunto de técnicas, las cuales puedes ser adaptables a las necesidades de la investigación. Para la realización de dicha investigación se ha tomado en cuenta 7 capítulos, los cuáles se esquematizan de la siguiente manera:

En el capítulo I, se presenta los problemas de seguridad de la información de las diferentes áreas de la Clínica Internacional – Piura (CI), argumentando la necesidad e importancia del desarrollo de la presente investigación, la cual se sustenta en antecedentes y bases teóricas, definiendo los objetivos de la investigación.

En el capítulo II, se detalla todo lo concerniente al método utilizado incorporando el diseño y tipo de investigación, definiendo las dimensiones e indicadores, población, muestra y las técnicas e instrumentos necesarios para lograr los objetivos plasmados.

En el capítulo III, se exhiben los resultados obtenidos después de efectuar el análisis de riesgo, empleando gráficos estadísticas que permitirán una mejor visualización e interpretación; los mismos, serán discutidos en el capítulo IV, siendo contrastados con teorías y antecedentes indagadas.

En el capítulo V, se presenta como dicha investigación ha cumplido con los objetivos propuestos al inicio de esta investigación, así mismo en el capítulo VI, se muestran algunas recomendaciones en relación a análisis de riesgos.

Para terminar en el capítulo VII se detalla la propuesta para salvaguardar los activos de información de Clínica Internacional – Piura.

ÍNDICE

RESUMEN

La presente investigación fue desarrollada a la Clínica Internacional – Piura, con la finalidad de aplicar la metodología MAGERIT para describir su situación actual de los riesgos de los activos de información.

Esta investigación es de tipo descriptiva. No obstante, se utilizó una muestra de 84 activos identificados clasificados por su tipología correspondiente. Asimismo, se aplicó la metodología MAGERIT (2012), misma que permitió llevar acabo el análisis de riesgos, teniendo en cuenta algunas características de la ISO 27002:2013, cuyo análisis permitió desarrollar una propuesta de salvaguardas y/o controles para mitigar los riesgos identificados.

Para alcanzar los objetivos fue importante la utilización de distintos instrumentos como fichas de registros, cuestionarios y fichas de observación, muchos de los cuales los brinda la metodología aplicada pero que fueron adaptados a la necesidad de la organización en estudio.

Finalmente se obtuvo la situación actual de la organización dando como resultado que Clínica Internacional – Piura con las salvaguardas existentes se encuentra en un nivel medio de riesgo. Esto, aprueba la hipótesis propuesta; es decir, la metodología MAGERIT permite describir la situación actual de la Clínica internacional – Piura en relación a los riesgos de los activos de información.

Palabra Clave: Metodología MAGERIT, ISO27002, Activo, amenaza, vulnerabilidad, riesgos, salvaguardas.

ABSTRACT

This research was developed at the International Clinic - Piura, in order to apply the methodology MAGERIT to describe the current situation of the risk of information assets.

This research is descriptive. However, a sample of 84 identified assets classified by their corresponding type was used. Also, the MAGERIT methodology (2012) was applied, it allowed carry out risk analysis, taking into account some features of the ISO 27002: 2013, whose analysis allowed to develop a proposal for safeguards and / or controls to mitigate the risks identified.

To achieve the objectives was important to use different tools such as tabs records, questionnaires and observation sheets, many of which provides the methodology applied but were adapted to the needs of the organization under study.

As a result of research the current situation of the organization was obtained resulting in International Clinic - Piura with existing safeguards is at a medium level of risk. This approves the proposed hypothesis; ie the MAGERIT methodology allows describing the current situation of the International Clinic - Piura in relation to the risks of information assets.

Keyword: Methodology MAGERIT, ISO27002, active, threat, vulnerability, risks, safeguards.

I. INTRODUCCION

1.1 Realidad Problemática

En la actualidad, la información es un activo importante e integral para todo tipo de organización, y se encuentra inmersa en todos sus procesos de negocios ya sean manuales o automatizados.

Mantilla, y otros (2003), hacen mención que la información pasa por un proceso que se lleva a cabo mediante sistemas cuya existencia incrementan la cantidad de información procesada y generada al igual que las amenazas a los que los activos de información están expuestos, es aquí que Merino, y otros (2011), mencionan que desde la antigüedad se era consciente de la existencia de amenazas a las que la información estaba expuesta; por ende, se utilizaban medios para protegerlos ya que podían ocasionar pérdidas de tiempo, dinero y dificultades operacionales. Así mismo, Aguilera (2010), indica que ciertas amenazas a los diferentes activos de información de una empresa pueden afectar la continuidad del negocio.

Como lo mencionan Ramos, y otros (2002), la destrucción, copia o pérdida de la información que se genera en una organización, acarrean consecuencias graves para la misma, lo que conlleva a requerir procedimientos de seguridad para su protección o la reducción del impacto de dichas amenazas.

Correa (2009) menciona que la finalidad de la seguridad de la información es proteger los 3 pilares o dimensiones fundamentales de la información denominados: Confidencialidad, Integridad y Disponibilidad, quienes en muchas ocasiones son afectados por distintas amenazas, concepto reforzado por Segunda Cohorte (2014), que considera que la seguridad de la información son mecanismos que resguardan y protegen dichos pilares.

Clínica Internacional (CI) Sede Piura es una organización dedicada al rubro de Salud, ubicada en la ciudad de Piura, actualmente cuenta con 26 especialidades complementándose con un staff médico y asistencial competente, además de ello es una organización en constante crecimiento, en cuando a servicios, pero también en cuanto al incremento de información que se genera, de ahí la necesidad de tomar conciencia de la importancia del aseguramiento de su

información que le permita superar las deficiencias actuales en cuando a la seguridad de los activos.

En CI ya se han dado situaciones de pérdida de información valiosa, ya que no existen procedimientos para evitar ingresos de dispositivos, accesos no autorizados y ni la clasificación de los activos de información por grado de sensibilidad ni criticidad, atentando con la seguridad de los activos de información que son de suma importancia para la organización.

La norma ISO/IEC 27002, que es un estándar que provee un conjunto de buenas prácticas para gestionar los riesgos y brindar seguridad, recomienda que las organizaciones deberían contar con controles de entrada adecuados para la protección de las distintas áreas, donde sólo el personal autorizado tendría acceso. A la vez indica que *"la información debería estar clasificada para saber cuan sensible y crítico puede llegar hacer el daño que cause la materialización de una amenaza para la organización" (*ISO/IEC 27002*)*

En la clínica en estudio se han presentado inconvenientes en sus operaciones, afectando a los pilares de la información ya que ocasionalmente la red se congestiona, y frente a una falla eléctrica muchos de los equipos de trabajo de los colaboradores pierden información, puesto que no poseen las medidas necesarias para prever este inconveniente, ni se tiene el conocimiento de las vulnerabilidades que tienen los activos de información, perjudicando la continuidad del negocio, y la dimensión de disponibilidad. Como indica la ISO/IEC 27002, *"se debe evaluar el grado de exposición de la organización en relación a las vulnerabilidades técnicas a las que se encuentra expuestos los activos de información, para poder salvaguardarlos y evitar o minimizar el riesgo".*

CI atraviesa muchos inconvenientes en relación al manejo de la información como por ejemplo la existencia de carpetas compartidas, que están a disposición de todo el personal que tenga acceso a la red, lo que conlleva a problemas tanto económicos como de imagen, ya que como indica la Ley N° 29733 de Protección de Datos Personales, *"toda organización debe garantizar la privacidad de la información que abarque el ámbito de la vida de las personas naturales".*

En esta investigación se busca realizar un análisis de la condición actual de las amenazas, vulnerabilidades y riesgos a la que están expuestos los activos de información de esta organización aplicando la metodología MAGERIT.

Con el análisis de los activos de información, que permite tipificarlos, valorarlos y a la vez identificar sus amenazas, vulnerabilidades y riesgos, se busca garantizar la protección de todos los activos de la misma y mejorar la seguridad de la información y la continuidad de sus operaciones estableciendo las salvaguardas adecuadas.

1.2 Trabajos Previos

Dentro de los trabajos previos de análisis de riesgo en organizaciones, tenemos:

- La tesis denominada **"Evaluación de la seguridad de las tecnologías de la información en la empresa Consolidated Group Del Perú SAC Basado En NTP-ISO/IEC - 17799-2007"** desarrollada por Nieves Benites, Daysi Sharon. (Piura, 2013), que tuvo como objetivo principal el "*elaborar las narrativas de prueba de cada uno de los controles de seguridad de la información que se requerían establecer para que el centro de procesamiento de datos de dicha empresa cumpla con las buenas prácticas de la norma técnica peruana NTP- ISO/IEC 17799-2007"*. Esta investigación es de un paradigma cuantitativo y diseño cuasi-experimental, que consideró una muestra de 6 personas del área de Tecnologías de información. Como resultado del pre-test y post-test, se elaboró la propuesta de diferentes controles, por esto la autora concluye que, con la aplicación de la norma NTP – ISO/IEC 17799:2007 y la implementación de documentos de control entre ellos: "Revisión de políticas", "Asignación de Activos informáticos", "Control de activos Informáticos", "Procedimientos para la administración de incidentes", "Procedimiento para la Continuidad de operaciones del centro de procesamiento de datos", "Formato identificación de Procesos Críticos para ser considerados en el Plan de Contingencias", entre otros, se mejora la evaluación de la seguridad de las tecnologías de la información en la empresa Consolidated Group del Perú SAC".

- La Tesis denominada **“Plan de contingencia en seguridad de tecnologías de información, basándose en la ISO 27031 para la municipalidad Distrital de Tambogrande“** elaborada por Riofrio García, Carlos David (Piura, 2014), quien indica que un plan de contingencia es de suma importancia para toda empresa, ya que si se da algún suceso, las actividades de la misma se reestablecerían lo más antes posible sin ningún inconveniente, tomando como objetivo principal en su investigación el de reducir las incidencias de tipo natural, física y lógica en la municipalidad Distrital de Tambogrande. Esta investigación se encuentra enmarcada en el contexto de paradigma cuantitativo, dentro del cual se define una investigación descriptiva, considerando una muestra de 20 directivos de las diferentes áreas pertenecientes a la municipalidad. Dentro de las conclusiones resaltantes, el investigador citó que *“Gracias al análisis que se realizó a la situación actual de la organización, se pudo lograr implementar el plan de contingencia que incluyó un plan de reducción, de recuperación y de respaldo de la información”*

- Perafán Ruiz, John Jairo y Caicedo Cuchimba, Mildred (Popayán, 2014) elaboraron su proyecto de tesis **“Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca (IUCMC)”.** Su objetivo principal fue realizar el análisis de riesgos, para finalmente proponer los controles que se necesiten para minimizar riesgos que se encuentran asociados con las vulnerabilidades y amenazas existentes en la institución Universitaria. Esta investigación es de tipo aplicada, considerando que dicho estudio busca una posible solución de lo que se conoce y de lo que no. Uno de los resultados principales que describen los autores es que *“Los controles son adaptados de acuerdo al resultado sobre estimación de riesgo teniendo en cuenta las necesidades y características de cada activo”*, a la vez concluyeron que “a*plicar la metodología MAGERIT para el análisis de riesgo es el primer paso para garantizar la seguridad de los activos de información, el análisis de riesgo aplicado, permite*

conocer de manera global el estado actual de la seguridad informática dentro de la IUCMC. Por lo que los controles y políticas de seguridad de la información resultado de este análisis de riesgos pueden ser tomados como soporte para la implementación del SGSI".

- Quiroz, Jhon Henry y Forero Cruz, William (Bogotá, 2015) elaboraron su tesis denominada **"Diseño de recomendaciones de seguridad informática sobre los activos de información críticos de la empresa Gran Tierra Energy Colombia – Seccional Bogotá"**. El objetivo principal de esta tesis fue diseñar recomendaciones de seguridad informática sobre los activos de información críticos de la empresa en estudio en el área de IT, con el fin de protegerlos y mejorar condiciones actuales. Esta investigación es de carácter cualitativo, y utilizó técnicas e instrumentos como entrevistas, encuestas, análisis de documentos, matrices, etc. tomando una muestra de 15 funcionarios. Una de las conclusiones importantes que citaron los autores fue que luego de identificar y evaluar el sistema con y sin controles, los impactos de valor medio en la dimensión de la disponibilidad se redujeron a un 29%, pasando del 35% al 6%, indican que en la dimensión integridad los activos con valor irrelevante pasaron del 59% al 70% y los activos de un nivel alto pasaron a representar de un 21% a un 12%.

1.3 Teorías relacionadas al tema

Para poder entender la investigación es necesario conocer de algunas teorías en relación al tema, principalmente saber acerca de la metodología aplicada y en qué consiste.

MAGERIT es una metodología de analizar y gestionar riesgos, nace para proteger los activos de información y garantizar la confidencialidad, veracidad y la continuidad del negocio.
MAGERIT (2012), indica que dicha metodología es *"utilizada para analizar los riesgos derivados del uso de las tecnologías de la Información y comunicaciones para así implementar medidas de control adecuadas que permitan tener riesgos controlados."* Por lo que esta metodología, permite conocer el estado actual de una organización en relación a los riesgos al que están expuestos los activos de información y poder tomar decisiones de seguridad para contrarrestarlos.

Basado en lo que indica la metodología MAGERIT, y sustentado por Correa (2009), la seguridad de la información busca proteger de la manera más adecuada la confidencialidad, integridad y disponibilidad, los cuales son conocidos como los 3 pilares de la información o dimensiones de la seguridad de la información, definidos de la siguiente manera:

- ***"Confidencialidad**.- Condición que garantiza que la información es accedida sólo por las personas autorizadas según la naturaleza de su cargo o función dentro de la organización*
- ***Integridad.**- Característica de la información que garantiza que la información sigue siendo veraz.*
- ***Disponibilidad.**- Característica de la información que garantiza que puede ser accedida en el momento en que es requerida".*

La definición de lo que es un análisis de riesgo es fundamental ya que es parte de los objetivos a lograr. Este concepto basado en lo que menciona el Instituto Nacional de Tecnologías de la comunicación (INTECO), *"es un proceso que consiste en identificar los riesgos de seguridad en nuestra*

empresa, determinar su magnitud e identificar las áreas que requieren implantar salvaguardas, se conocerá el impacto de un fallo de seguridad y la probabilidad realista de que ocurra este fallo." MAGERIT (2012), señala que "*es un proceso sistemático para estimar la magnitud de los riesgos a lo que está expuesta una organización".* Dicha metodología proporciona distintas actividades a seguir para lograr un análisis de riesgos que permitirá identificar las amenazas, vulnerabilidades y los riesgos de los activos de información, pudiendo implantar salvaguardas para proteger dicho activos. Es aquí que Escrivá (2013), menciona que *"Hay que tener en cuenta qué activos hay que proteger, sus vulnerabilidades y amenazas, así como la probabilidad de que estas se produzcan junto con el impacto de las mismas".* El resultado de un análisis de riesgos permite recomendar medidas para la protección de los activos de información.

MAGERIT, estudia los riesgos y recomienda las medidas necesarias para brindar un sistema de información seguro. Por tanto se divide en el análisis y el tratamiento. En el análisis de riesgos, la metodología MAGERIT plantea las diferentes tareas como se observa en la figura N°01

Fuente: Metodología MAGERIT (2012)
Elaboración propia
Figura N° 01: Análisis de riesgo según MAGERIT

Para la metodología MAGERIT el primer paso consiste en identificar los activos de información por tipología, asimismo la importancia que tiene cada uno de ello, cuyos valores se encontraran en un escala del 1 al 5, la misma que definirá cuan crítico es el activo.

Escrivá (2013), considera que un activo *"es aquel recurso del sistema (informático o no) necesario para que la organización alcance los objetivos propuestos; es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, ya sea intencionado o no."* Y según Tejada (2015), la importancia del activo dependerá de su valor.

Los activos son elementos indispensables para una entidad, pueden ser de mucho o poco valor, pero que consisten en una inversión dada por la organización, por tanto, es necesario su adecuada y pronta protección para que sus negocios no sean perjudicados.

MAGERIT tipifica los activos como los elementos de TI a proteger dentro de la organización como se aprecia en la figura N° 02

Fuente: Metodología MAGERIT (2012)
Elaboración Propia
Figura N° 02: Tipificación de activos de información.

Para la valoración estimada de los activos **[VE]**, la metodología aplicada indica que puede ser cualitativo o cuantitativa y se deben tener en cuenta los pilares de la información, y las diferentes preguntas que abarcan cada uno de ellas:

- ***"[C] Confidencialidad:*** *¿qué daño causaría que lo conociera quien no debe?*
- ***[I]Integridad:*** *¿qué perjuicio causaría que estuviera dañado o corrupto?*

- ***[D]Disponibilidad:*** *¿qué perjuicio causaría no tenerlo o no poder utilizarlo?"*

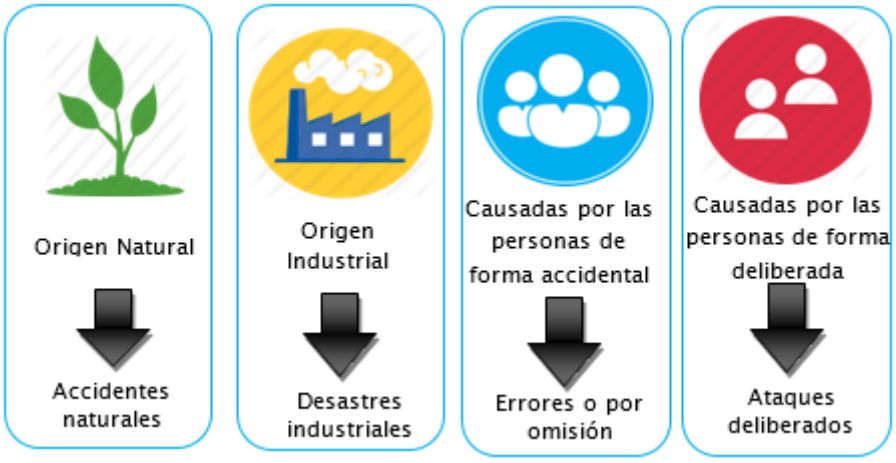
El valor estimado de los activos es el promedio del valor de las tres dimensiones

$$VE = (C + I + D)/3$$

El siguiente paso de la Metodología MAGERIT es determinar y valorar las amenazas que pueden atentar contra la seguridad de los activos de información.

Escrivá (2013), define una amenaza a "*cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático. Aunque hay amenazas que afectan a los sistemas de forma involuntaria, como, por ejemplo, un desastre natural, en la mayoría de casos es necesaria una intención de producir daño".*

MAGERIT clasifica las amenazas como los eventos que se pueden presentar, como se observa en la figura N° 03.



Fuente: Metodología MAGERIT (2012)
Elaboración propia
Figura N°03: Clasificación de amenazas a los activos de activos de información.

Dicha clasificación, permite la facilidad de la identificación de las amenazas a las que está expuesta cada activo, teniendo en cuenta que diferentes amenazas afectan distintos activos. Se valora teniendo en cuenta la probabilidad de ocurrencia que indicará la probabilidad de que se materialice la amenaza y la degradación del activo donde influye cuan perjudicado resultaría el valor del activo, valorado en porcentaje.

Las escalas de valor estimado, probabilidad de ocurrencia y la degradación se muestran en la tabla N° 01:

ESCALA	[VE]		[P]		[D]	
	VALOR	Descripcion	VALOR	Descripcion	%	Descripcion
MB = Muy Bajo	1	Irrelevante a efectos practicos	1	Cada varios años	10%	Degradación muy baja del activo
B = Bajo	2	Daño menor	2	Hasta 2 veces al año	30%	Degradación baja del activo
M = Medio	3	Daño Importante	3	Hasta una vez al año	50%	Degradación media del activo
A = Alto	4	Daño grave	4	Hasta una vez al mes	80%	Degradación alta del activo
MA = Muy Alto	5	Daño muy grave	5	Mas de una vez al mes	100%	Degradación muy alta del activo

Fuente: Metodología MAGERIT (2012)
Tabla N° 01: Escala de valoraciones

Dentro de este paso, MAGERIT considera el cálculo del impacto potencial y del riesgo potencial.

Para MAGERIT (2012), el impacto es "*la medida del daño sobre el activo derivado de la materialización de una amenaza",* una vez valorado los activos de información (en sus 3 dimensiones) y la degradación, se puede obtener el impacto que tendrían sobre los activos.

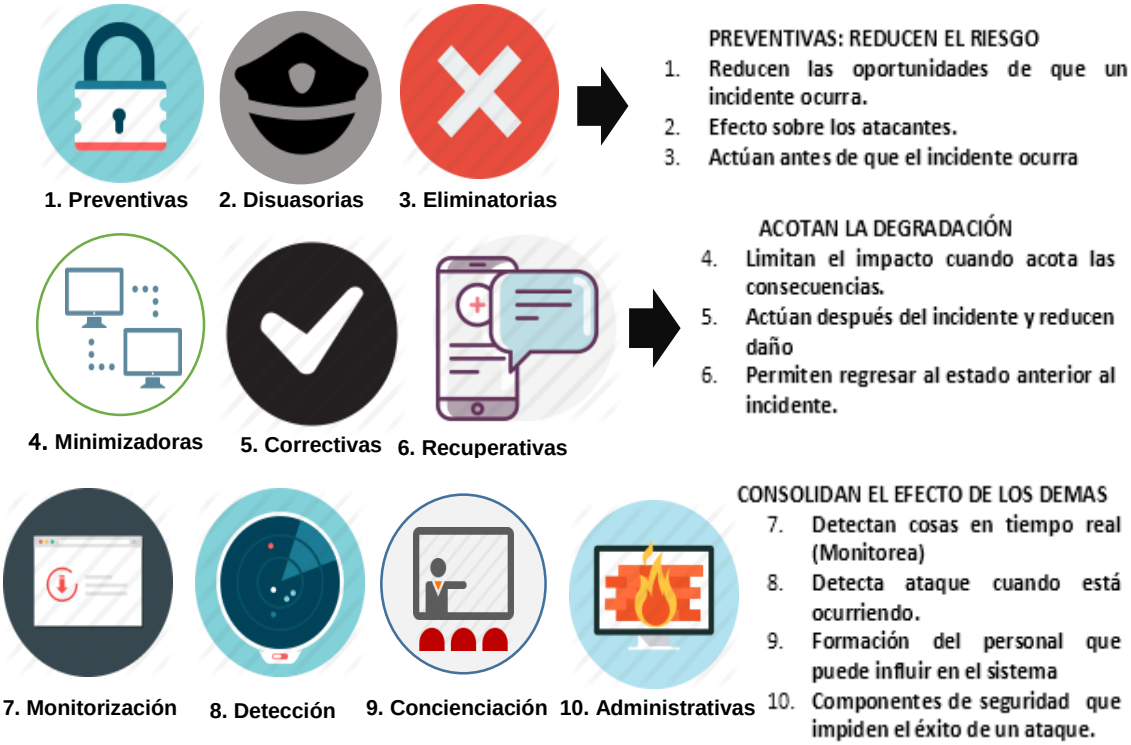
MAGERIT (2012), también considera que "*el riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente".* Por lo tanto es importante conocer las características que conforma un análisis de riesgos es decir identificar las amenazas, vulnerabilidades, de los activos de información y saber la medida de peligro a los que están expuestas.

En el paso 3 se caracterizan las vulnerabilidades, definidas por MAGERIT (2012), como "*las debilidades que pueden ser aprovechadas por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial."*

Al igual que los activos, las vulnerabilidades deben valorarse, pero antes, deben identificarse y evaluarse tomando como criterio la probabilidad de explotación.

La última etapa de la metodología aplicada considera la caracterización de las salvaguardas, controles o contramedidas, las cuales son definidas por Areitio (2008),como *"procedimientos o dispositivos físicos o lógicos que pueden proteger o controlar una amenaza, reducir la vulnerabilidad, limitar el impacto de un incidente no deseado y facilitar la recuperación.",*

La clasificación de las salvaguardas propuestas por MAGERIT se observa en la figura N° 05.



Fuente: Metodología MAGERIT (2012)
Elaboración propia
Figura N° 05: Clasificación de Salvaguardas.

Las salvaguardas se caracterizan por su eficacia de protección, en un rango del 0% para las inexistentes y el 100% eficacia perfecta.

ESCALA	EFICACIA [E]	
	VALOR	DESCRIOPCION
L5 = Optimizado	100%	Mejora continua
L4 =Gestionado y Medible	90%	Monitorizado
L3 = Procesado y medible	70%	En Funcionamiento
L2 = Reproducible, pero intuitivo	40%	Parcialemnte realizado
L1 = Inicial/ ad hoc	10%	iniciado
L0 = Inexistente	0%	Inexistente

Fuente: Metodología MAGERIT
Tabla N° 02: Escala de valoración de Salvaguardas.

Para la determinación de los indicadores de riesgo, MAGERIT propone utilizar las siguientes relaciones matemáticas:

- Degradación **[D],** probabilidad de ocurrencia de la amenaza **[P]**, impacto potencial **[IP]** y riesgo potencial **[RP]:** Que vienen hacer aquellas valoraciones que no toman en consideración salvaguardas.

- El cálculo del impacto potencial resultará de la multiplicación del resultado del valor de los activos **[VE]** por la más alta valoración de degradación de la amenaza en cada uno de las dimensiones y el cálculo del riesgo potencial se obtendrá de la multiplicación del impacto potencial por la probabilidad de ocurrencia.

- Degradación Residual **[DR],** Probabilidad Residual de ocurrencia de la amenaza **[PR]**, Impacto Residual **[IR]** y Riesgo Residual **[RR]:** son aquellas valoraciones que toman en consideración salvaguardas. Para su cálculo se debe haber evaluado primero la eficacia de la salvaguarda **[E]**, teniendo en cuenta que afecta a la degradación y la probabilidad
  - La degradación Residual es la resta entre eficacia perfecta (100%) y la eficacia real de dicha salvaguarda.
  - Probabilidad residual de ocurrencia de la amenaza es igual a la probabilidad por la degradación residual.
  - El impacto residual es la multiplicación del Impacto potencial por degradación residual.
  - El riesgo Residual es la multiplicación del impacto residual por probabilidad residual de ocurrencia de la amenaza.

IP =VE * MAX (D) **RP = IP * P**	**DR = 100% - E** **PR = P * DR**	**IR=IP * DR** **RR=IR * PR**

Después de la estimación del riesgo, se realiza su debido tratamiento, proponiendo controles para las salvaguardar los activos de información, tomando como guía la norma ISO/IEC 27002:2013.

1.4 Formulación del Problema

1.4.1 Pregunta General.

- ¿Cuál es la situación actual de los riesgos de los activos de información identificados en la Clínica Internacional – Piura aplicando la metodología MAGERIT?

1.4.2 Preguntas Específicas.

- ¿Qué activos de información posee la Clínica Internacional – Piura aplicando el análisis de riesgos de la metodología MAGERIT?
- ¿Cuál es la caracterización de las amenazas identificadas en los activos de información aplicando la metodología MAGERIT?
- ¿Cuál es la caracterización de las vulnerabilidades existentes en los activos de información de la Clínica Internacional - Piura aplicando la metodología MAGERIT?
- ¿Cuáles son las salvaguardas de los activos de información de la Clínica Internacional – Piura aplicando la metodología MAGERIT?

1.5 Justificación del Estudio

De acuerdo a la problemática planteada al inicio de esta investigación y acorde a los objetivos plasmados, la investigación se justifica ya que para el cumplimiento de los mismos, se hace uso de la metodología "MAGERIT" quien brinda los pasos necesarios para el análisis de riesgos de los activos de información, permitiendo usar distintos instrumentos como fichas de registro y cuestionarios, debido a que posee un método sistemático para su estimación y análisis, beneficiando a personas que requieran realizar un análisis de riesgos de los activos de información. De igual manera la metodología MAGERIT posee como objetivo crear una cultura de conocimiento acerca de la existencia de riesgos y la necesidad de contenerlos a tiempo, lo cual se plasma como una necesidad según la problemática antes mencionada, no solo para la organización en estudio, también para las distintas organizaciones. Además esta investigación es de suma importancia para todo tipo de entidad, debido a que permite ejercer conocimientos sobre análisis, control y resguardo, de los activos

de información más relevantes propios de la misma, permitiéndole minimizar futuras pérdidas económicas, de imagen, entre otras. En este caso la Clínica Internacional sede Piura podrá conocer su situación actual en relación a riesgos de sus activos de información, para protegerlos y evitar pérdidas ya antes mencionadas.

1.6 Hipótesis

"La metodología MAGERIT describe la situación actual de los riesgo de los activos de información de la Clínica Internacional – Piura”

1.7 Objetivos

1.7.1 Objetivo General

- Analizar los riesgos de los activos de información identificados en la Clínica Internacional – Piura aplicando la metodología MAGERIT.

1.7.2 Objetivo Específicos

- Identificar y valorar los activos de información de la Clínica Internacional – Piura de acuerdo a la Metodología MAGERIT.
- Determinar y analizar las amenazas identificadas en los activos de información de la Clínica Internacional - Piura aplicando la metodología MAGERIT.
- Determinar y analizar las vulnerabilidades existentes en los activos de información de la Clínica Internacional - Piura aplicando la metodología MAGERIT.
- Proponer las salvaguardas para los activos de información de la Clínica Internacional – Piura aplicando la metodología MAGERIT.

II. MÉTODO

2.1. Diseño de Investigación.

El tipo de investigación es descriptiva ya que permite caracterizar los activos de información de la clínica Internacional – Piura, identificado sus amenazas, vulnerabilidades y riesgos con el fin de proponer salvaguardas para su protección.

De acuerdo a los estudios descriptivos tenemos: $\boldsymbol{O - M}$

0 = Observación de M, aplicando la Metodología MAGERIT

M = Análisis de riesgos de los activos de información

2.2. Variables, Operacionalización.

Variable: Análisis De Riesgos de los Activos de Información

VARIABLES	DEFINICIONES		DIMENSIONES	INDICADORES
	CONCEPTUAL	OPERACIONAL		
ANALISIS DE RIESGOS DE LOS ACTIVOS DE INFORMACION	Según MAGERIT (2012), *"Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización".*	Esta variable se medirá usando Fichas de registro proporcionada por la metodología MAGERIT, las cuales han sido adaptadas a la realidad de la organización, objeto de estudio. Así mismo se utilizarán encuestas.	Activos	Tipo de Activo
				Valoración estimada
			Amenaza	Tipo de amenaza.
				Degradación
				Probabilidad de Ocurrencia
				Impacto potencial y residual
				Riesgo potencial y residual
			Vulnerabilidad	Tipo de vulnerabilidades.
				Probabilidad de explotación
			Salvaguardas	Tipo de Salvaguardas
				Valoración Estimada

Tabla N°03: Cuadro De Operacionalización De Variable/Indicadores del Análisis de Riesgo de la Información de Clínica Internacional – Piura Aplicando la Metodología MAGERIT.

2.3. Población y muestra.

Las unidades de análisis que se emplean en este estudio se encuentran:

- Los activos agrupados según la clasificación de la metodología aplicada, forman una población de 676 activos de información.
- El personal son aquellos colaboradores de la organización en estudio (en un total de 231), que tienen una interacción con los activos de información que serán estudiadas para medir el nivel de conocimiento respecto a seguridad.

El tipo de muestra es no probabilística y el criterio de selección es por conveniencia, ya que la metodología MAGERIT, permite agrupar los activos de similares características dejando solo un activo genérico o los de mayor valor para la organización reduciendo la cantidad de la muestra utilizada a 84 activos de información. Así mismo, en la unidad de análisis personal por disponibilidad del mismo, se redujo a una muestra de 61 personas.

UNIDAD DE ANÁLISIS	Población	Muestra
Activos	**676**	**84**
Personal	**231**	**61**

2.4. Técnicas e instrumentos de recolección, validez y confiabilidad.

2.4.1. Técnicas.

Análisis de documento: Esta técnica se utilizó para encontrar información valiosa y necesaria de la organización que permitió cumplir con los objetivos propuestos

Encuesta: Técnica utilizada para la recopilación de información necesaria para toda la investigación, realizando una serie de preguntas al personal de la organización que fue base fundamental para el análisis de riesgos.

2.4.2. Instrumentos.

Ficha de Registro: Son aquellos formatos basados en la metodología MAGERIT adaptados a la necesidad de la organización, utilizados para la recopilación de datos, e información de las valoraciones de los activos, amenazas, vulnerabilidades, salvaguardas y riesgos.

Cuestionario: Es un instrumento que se aplicó para valorar el activo de tipo personal en los tres pilares de la información, así como para medir los indicadores necesarios para el análisis de riesgos e identificación de salvaguardas desplegables (existentes) en la organización.

Técnicas	Instrumentos
Análisis de documento	**Ficha de registro**
Encuesta	**Cuestionario**

La validación y confiabilidad de los instrumentos utilizados para medir los indicadores, se ha realizado a través de la evaluación de dos jueces expertos, quienes han revisado el contenido de los mismos, evaluándolos y asegurando su alcance para lograr los objetivos planteados en esta investigación.

2.5. Método de análisis de datos.

Para la realización de los instrumentos se ha hecho uso de la herramienta Microsoft Excel, que contiene distintas hojas de cálculo y fórmulas que facilitaron el procesamiento de datos estadísticos, empleando tablas de contingencia, diagrama de barras, y gráficos de sectores para sus representaciones gráficas.

2.6. Aspectos éticos.

Los fines de la presente investigación, autorizada por la Clínica Internacional - Piura por medio de un documento de conformidad, son netamente académicos, por lo que se ha brindado a la organización, la seguridad de la confidencialidad de la información utilizada en la presente investigación.

III. RESULTADOS

De acuerdo a los objetivos planteados en la investigación, se muestran los resultados en base a las dimensiones (activos, amenazas, vulnerabilidades y salvaguardas) de la variable en estudio *"Análisis de riesgo de los activos de información".*

En relación a la dimensión activos, uno de los indicadores evaluados fue identificar y tipificar los activo que se encontraban en la organización obteniendo que la tipología datos/información y redes de comunicación fueron aquellos que representaron la mayor y menor cantidad de activos en la organización (18% y 5%), como se muestra en el gráfico N°01.

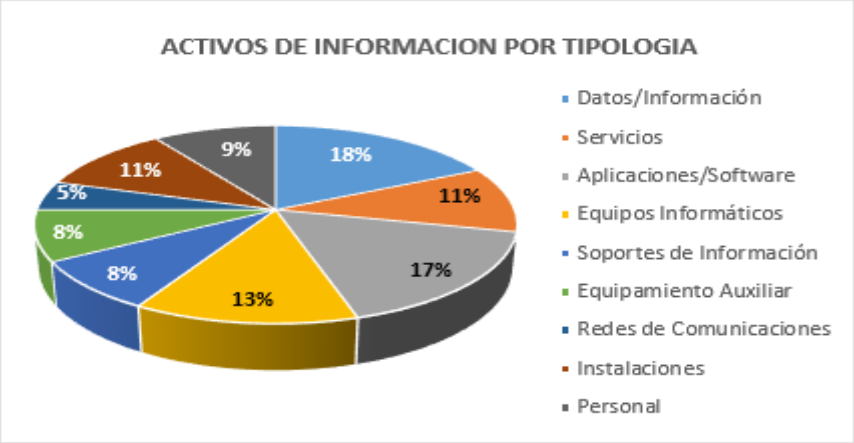


Gráfico N° 01: Medición del indicador tipos de activos de la dimensión activos

Con el primer indicador se pudo obtener la valoración estimada de dichos activos, el mismo que viene a ser el resultado del valor asignado en cada uno de los pilares de la información (integridad, disponibilidad y confiabilidad), cuyo valor se obtuvo aplicando la técnica Delphi y comprobándose con un 95% de confianza que el tipo de activo es un factor determinante para dicha valoración, reflejando que los activos de mayor y menor valoración, fueron los de tipo soportes de información y los activos de redes de comunicaciones con un valor estimado de 4.6 y 3.5 respectivamente(Ver anexo 11).En conjunto los activos de información se ubican entre un nivel alto y un nivel medio de valoración. (43% y 18%), evidenciando que los usuarios tienen conocimiento de la importancia y criticidad que tienen los activos con los que ellos interactúan, sin embargo la falta de salvaguardas implantadas en la organización los ponen en riesgos.

Otra dimensión importante son las amenazas que engloba un conjunto de indicadores que permiten determinar el impacto y riesgo al que está expuesto la organización, uno de los cuales lo conforma la identificación de las amenazas, para la cual se empleó y adaptó el catálogo que brinda la metodología MAGERIT (2012) obteniendo como resultado que, errores y fallos no intencionados representan la mayor cantidad de amenazas con un porcentaje de 45% (Ver Anexo N° 12), lo cual hace referencia a la falta de concientización de la organización para con sus empleados (usuarios) a cerca del buen uso, manejo y manipulación de sus activos.

Respecto al indicador degradación, se obtuvo mediante la técnica Delphi el porcentaje de cuan perjudicado resultaría el valor del activo si una amenaza lo afectara, sin contar con medidas de seguridad, obteniendo que el 61% de los activos representan una degradación muy alta de su valor, de los mismo que aplicaciones/software y soportes de información resultarían aún más perjudicados en un 98% y 95% respectivamente (Ver Anexo N° 13). De acuerdo a la probabilidad de ocurrencia se obtuvo que los activos de información tienen una probabilidad muy alta de que ocurran dichas amenazas identificadas (52%), siendo los más probables los de tipo de activos datos/información, aplicaciones/software y personal (Ver Anexo N° 14)

Según los datos recolectados se pudo determinar el impacto y riesgo potencial, cuyos resultados mostraron que el valor de ambos se encontró en un nivel alto, siendo el impacto, el daño que causa al activo el que se materialice una amenaza, y el riesgo, la representación de lo que podría pasar a los activos de información si no tienen una protección adecuada, se obtiene que el tipo del activo es un factor determinante para el nivel de impacto con un grado del 95% de confianza, siendo los de tipo datos/información, equipos informáticos, aplicaciones/software los que representan un nivel alto de impacto y riesgo potencial adicionalmente de los servicios y personal como se presenta en el gráfico N° 02.

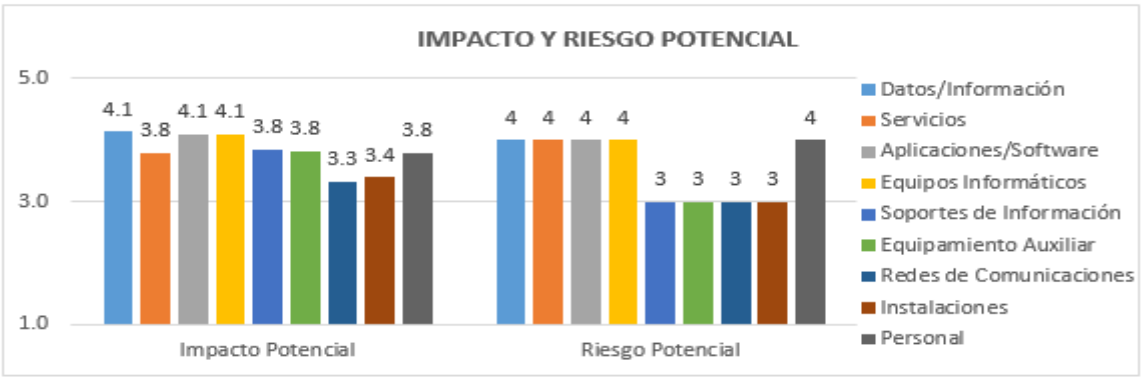


Gráfico N° 02: Medición de los indicadores impacto y riesgo potencial de la dimensión amenazas.

Con relación a la dimensión vulnerabilidad, se puede conocer cuáles son las debilidades que tiene la organización y cuál es la probabilidad de que una amenaza la explote, se observó que existe un mayor porcentaje en las vulnerabilidades de tipo seguridad física y ambiental (33%), y que existe una probabilidad muy alta (43%) siendo en su mayoría los activos más expuestos los de tipo aplicaciones/ software (con una probabilidad de 4.55). esto debido a que existe un cierto grado de inexistencia de salvaguardas para asegurar sus activos. (Ver Anexo N° 15)

En la investigación se resalta la importancia de las salvaguardas, encontrándose en un nivel muy bajo de eficacia, las salvaguardas desplegables (existentes), esto dado que, la organización no posee las salvaguardas adecuadas o muchas de ellas se encuentran en un porcentaje acorde a su escala de valoración que indica entre un nivel iniciado y reproducible, como se muestra en el gráfico N° 03.

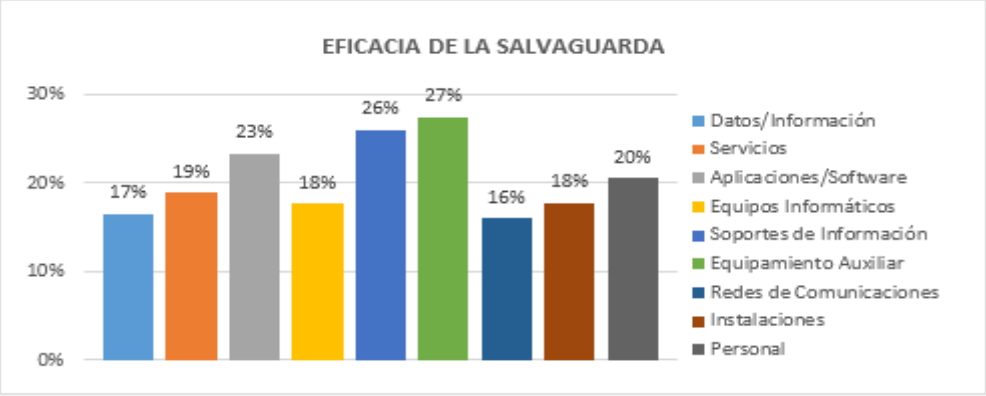


Gráfico N° 03: Medición del indicador eficacia de la dimensión salvaguardas

Con las salvaguardas actualmente implantadas, se pudo obtener la degradación y probabilidad de ocurrencia residual, así mismo el impacto y riesgo residuales. En relación a la degradación residual se obtuvo, que los resultados pasaron de un 98% a 86%, los mismo que mostraron casi ningún cambio positivo ya que dicho porcentaje sigue siendo una degradación de valor alto, con este nuevo análisis se exponen a una mayor pérdida de su valor, los activos de tipo personal (92%), los mismo que son los que tienen un mayor valor en la organización. (Ver Anexo N° 16)

Aún en el enfoque de la dimensión de las salvaguardas es importante determinar el impacto y riesgo residual, cuyos resultados de ambos se encontraban en un nivel medio aún con salvaguardas, representando los activos con un nivel alto de impacto residual los datos/información (3.8) y los que representan un nivel medio de riesgos residuales son datos/información, servicios, aplicaciones/software, equipos informáticos, soportes de información y personal, con un valor de 3, así como se muestra en el grafico N°04.

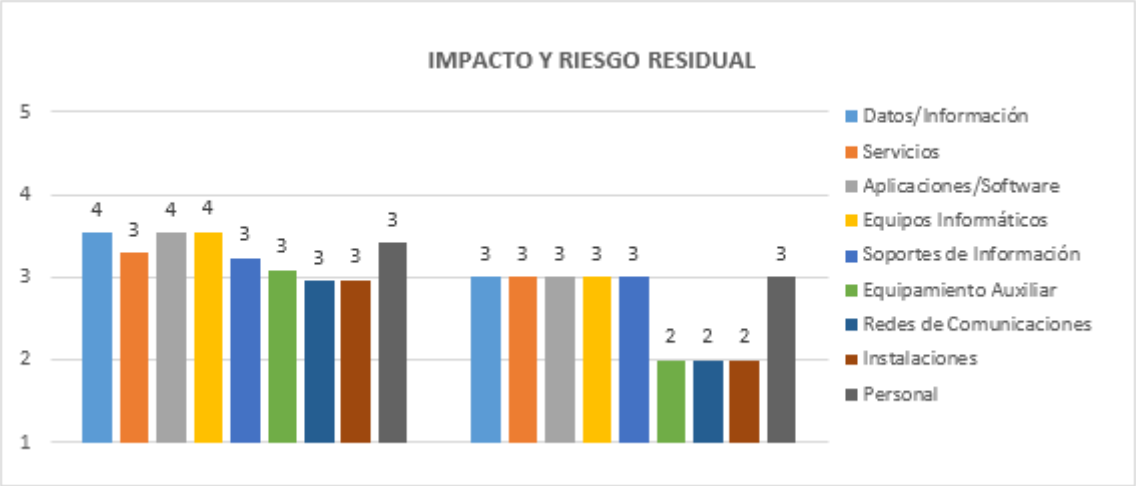


Gráfico N° 04: Medición de los indicadores impacto y riesgo residual de la dimensión amenazas.

Finalizado y obtenido los resultados de investigación se puede percibir que Clínica Internacional – Piura se encuentra en un nivel medio de riesgo ya que sus salvaguardas no son tan eficiente dado que muchas de ellas se encuentran en un nivel inicial., por lo cual es preciso proponer un plan de seguridad de los activos de la información que permitan, proteger a dichos activos.

IV. DISCUSION

El objetivo que tuvo la presente investigación es analizar los riesgos de los activos de información identificados en la Clínica Internacional – Piura aplicando la metodología MAGERIT, para ello se estudió las dimensiones de la variable en estudio.

Para un análisis de riesgos los activos de información es la primera tarea de realizar, cuyo indicador es su identificación y tipificación, permitiendo a la organización saber qué activos de información posee, y cómo están organizados por su tipología. Merino y otros (2011), indican que se debe conocer lo que se tiene para saber sus riesgos y tomar medidas para protegerlos, por lo que la identificación de los activos que posee la organización es el primer paso de esta metodología.

En su mayoría, las organizaciones cuentan con inventarios de activos cuya información es netamente de equipos informáticos, sin considerar otros tipos de activos que mellan o están relacionados con los procesos de negocio de las mismas como lo menciona MAGERIT (2012), cuya tipificación incluye adicionalmente la infraestructura, servicios, instalaciones, personal, entre otros, que son activos que permiten consolidar los procesos de negocio de la organización y que determinan el buen manejo y desempeño de la empresa. Así mismo Areitio (2008), concuerda con la metodología que los sistemas de información no solo se conforman por activos de hardware y software. En este estudio se tuvo una cantidad de 676 activos cuya agrupación y selección se redujeron a una totalidad de 84 activos de información, cuya investigación le permitió a la organización saber cuáles son los activos de información con los que cuenta.

Otro indicador definido como parte del estudio de los activos de información fue la valoración del mismo, MAGERIT (2012), indica, que los tipos de activos esenciales son datos/información y servicios, no obstante en esta investigación resulta que los soportes de información son los tipos de activo que poseen un valor de 4.6 a diferencia de datos/ información (4.3) y servicios (4.1) dando como resultado que los activos de alto valor no solo son aquellos activos esenciales, teniendo en cuenta que la valoración es brindada por aquellas personas que interactúan con el activo y dicho valor no será el mismo para todas las

organizaciones. En este caso en su mayoría las valoraciones obtenidas se encuentran en un nivel alto, dejando en evidencia que las personas y/o usuarios de la entidad tienen conocimiento de la importancia y criticidad de dichos activos tanto para ellos como para la organización, pero que por falta de procedimientos establecidos suelen ponerlos en riesgos. Nieves, Benites (2013) plantea en su tesis la importancia del uso de controles para mitigar y controlar los riesgos como lo son la implementación de documentos de control.

Otra dimensión importante del análisis de riesgos son las amenazas. Según la definición que plantea Merino, y otros (2011), las amenazas son acontecimientos o acciones que ponen en riesgo a la organización impidiendo su proceso y atentando contra su seguridad; en relacion a esta dimension se determinaron los tipos de amenazas, para MAGERIT (2012), existen cuatro; entre las cuales, amenazas naturales, origen industrial, errores y fallos no intencionales y ataques intencionales, en esta investigacion resultó que los errores y fallos no intencionados representan la mayor cantidad de amenazas en la organización con un porcentaje de 45%, implicando a las personas como una pieza importante para la seguridad de la información puesto que en este caso se sabe que existe el conocimiento de importancia del activo pero no se toman las medidas necesarias para protegerlos pudiendo generar una gran pérdida en la entidad. Así también se encuentran el tipo de amenaza ataques intencionados que representan el 35% de las amenazas, conociendo que esta es un punto difícil de controlar puesto que entra a tallar la parte de ética y moral, pero que se puede asignar algunas salvaguardas y/o controles que permitan proteger a los activos, mitigar y reducir los riesgos de este tipo de amenazas. Sin embargo también se resalta que es conveniente saber que no todos los activos de información son afectados por todas las amenazas pero que sí existe una relación entre el tipo de activo y lo que pueda ocurrir, sustento torico que lo respalda Merino, y otros (2011). Otro de los indicadores se encuentra la degradación del activo, cuya definición dada por MAGERIT (2012), indica que cuando una activo es víctima de una amenaza una parte de su valor se pierde, puede ser entre el 0% y un 100%, en este estudio se aprecia que los valores de degradación de los activos es muy alta (61%) esto implica que la organización puede tener grandes pérdidas económicas por causa de la materialización de las amenazas.

En relación a la probabilidad de ocurrencia, los resultados se ubicaron en un nivel alto (52%), debido a que se tomó en cuenta, los eventos ya sucedidos, al igual que el catálogo de amenazas por tipo de activos que brinda la metodología, mismo que resalta Merino, y otros (2011), quien nombra algunos catalagos de amanazas como los de la ISO/IEC2005, ISO/IEC27799,NIST, pero que destaca la que brinda la metodología aplicada.No obstante, es alarmante conocer que la organización esta muy propensa a que puedan suceder dichas amenazas, pero es bueno saber que con el analisis de riesgo se puede lograr distintos planes que permiten estar preparados ante ciertas eventualidades, como Riofrio García, Carlos David (2014), quienes afirman en su tesis que se pudo lograr implementar el plan de contingencia que incluyó un plan de reducción de riesgos, y un plan de recuperación y respaldo de la información.

En relación a esta dimensión también se plantearon como indicadores el impacto y el riesgo, cuyos resultados se determinaron de todo el análisis realizado sin evaluar ningún tipo de salvaguardas implantadas, teniendo en cuenta las probabilidades de ocurrencia de las amenazas, la degradación del activo y la valoración asignada a cada uno de las dimensiones de los activos identificados, que resultaron en conjunto en un nivel alto, dando que el impacto y riesgo potencial también se encuentren en dicho nivel, sabiendo que no se afecta de la misma manera a cada una de las dimensiones que el activo posee. En esta investigación, los resultados obtenidos demuestran que los tipos de activo en su mayoría presentan un nivel alto respecto al impacto y riesgo aumentando la necesidad de protegerlos y dando conocer a la organización el grado de riesgo en el que se encuentra expuesto, teniendo en cuenta que la información es una parte fundamental para que los procesos dentro de la entidad funcionen correctamente y se mantenga la fluidez de los servicios que brinda.

Según las vulnerabilidades detectadas se demuestra la existencia de muchas deficiencias, siendo muy propensas a que las amenzas las exploten, puesto que es bien cierto que las vulnerabilidades por si solas no causan daño pero, si cuando una amenza se aprovecha de ella, tal como lo afirma Merino, y otros (2011). Cabe resaltar que se encuentran muchas más vulnerabilidades en el tipo de seguridad física y ambiental, así como también en la del tipo seguridad ligada a recursos humanos. No obstante los resultados demuestran que es necesario

la implementación de salvaguardas que minimicen los riesgos que puedan causar pérdidas económicas y de imagen.

Por último en relación a las salvaguardas, de las cuales se han mencionado mucho anteriormente, son medidas de seguridad o de proteccion que una organización debe tener para con sus activos de información, como Perafán, John y Caicedo, Mildred (2014) plantea en su tesis la realizacion de un analisis de riesgos para generar controles que minimicen las probabilidades de ocurrencia e impacto de los riesgos asociandos a las vulnerabilidade y amenazas, obteniendo reducciones en las mismas. Para la obtención de resultados productivos a lo largo de toda el análisis de riesgos se realizó una identificacion de aquellas salvaguardas que ya estan implantadas hasta este momento en la organización, dando a conocer a la organización el riesgo actual de la misma, asi mismo el nivel de madurez (eficacia) que tienen dichas salvaguardas en su sistema de seguridad de la información. Uno de los indicadores que no se observa en sus resultados muchos cambios positivos fue el referido a las salvaguardas desplegadas. Los datos indagados detallan que en su mayoria las salvaguardas implantadas se ecuentran entre un nivel iniciado y reproducible, esto es consecuencia, probablemente, de no contar con las salvaguardas adecuadas, o que no se les da la importantacia necesaria, ya que no llevan una buena administración.

Sobre el impacto y riesgo residuales los resultados dieron que ambos se redujeron a un nivel medio comprobando que las salvaguardas son medidas que permiten mitigar, o reducir los riesgos a los que esta expuesto los activos de informacion que una entidad posee, Quiroz, Jhon y Forero, William (2015) afirman las mejoras que trae a una organización la implementacion de salvaguardas. Aunque en el estudio de dichos autores, su analisis fue dado en cada una de las dimensiones de informacion(confidencialidad, disponibilidad, integridad, autenticidad, y trazabiliadad), y en esta investigacion fue solo necesario optar por las 3 principales dimensiones de seguridad, ya que 2 de ellas se encuentran netamente relacionadas con estas, el impacto en su investigación se redujo en un 29% en la dimension disponibilidad.

Cabe resaltar que en esta investigación el riesgo e impacto disminuyeron a un nivel medio pero que la organización sigue estando en un nivel peligroso.

V. CONCLUSIONES

1. Al identificar y valorar los activos de información en la Clínica Internacional se pudo obtener que un 42% de los mismos, poseen un nivel de valoración muy alto, siendo los más importantes y críticos para la organización los activos de tipo datos/información (18%), dando a conocer que las personas que interactúan con dichos activos tienen conocimiento de su importancia, permitiéndole a la organización realizar planes de concientización acerca de la seguridad de los activos de información.
2. Respecto a las amenazas, se obtuvo que tienen una probabilidad muy alta de ocurrencia(52%), siendo las de tipos errores y fallos no intencionados las más usuales(45%), donde las personas son las más involucradas en este tipo de amenazas, estas amenazas identificadas pueden causar una pérdida muy alta del valor de los activos en su mayoría (61%), donde los activos de tipo datos/información son los más expuestos; estas valoraciones permiten obtener el impacto y riesgo potencial cuyos valores se determinaron en un nivel alto. Es alarmante saber que la organización esta muy propensa a que puedan suceder dichas amenazas, pero el beneficio que brinda el analisis de riesgo es realizar distintos planes que permitan estar preparados ante ciertas eventualidades.
3. En la dimensión vulnerabilidad, se consiguió conocer que la probabilidad de explotación se encuentra en un nivel muy alto (43%). Las vulnerabilidades de tipo seguridad física y ambiental, y las de tipo seguridad ligada a recursos humanos son las más frecuentes en la organización, siendo los tipos de activos aplicaciones/software los más vulnerables.
4. Sobre las salvaguardas, se logró identificar la eficacia de aquellas implantadas en la organización, dando como resultado que el más alto nivel de eficacia es de un 18% en los activos de tipo redes/comunicaciones, lo mismo que indica que su nivel de madurez está entre un nivel inicial y reproducible. Con las salvaguardas implantadas se redujo el impacto y riesgo a un nivel medio (pasando de un nivel alto a un nivel medio). Se concluye que al proponer nuevas salvaguardas y mejorar las ya establecidas el impacto y el riesgo pueden disminuir considerablemente.

VI. RECOMENDACIONES

Para lograr una mejora continua es necesario tener ciertas consideraciones determinadas al concluir con la investigación, las mismas que se describen a continuación.

- El presente estudio se desarrolló en base a la metodología MAGERIT, pero adicionalmente se tuvo en cuenta las buenas prácticas que brinda la ISO/IEC 27002; así mismo es recomendable seguir el ciclo de la ISO/IEC 27001 y someter a un análisis a los nuevos activos.

- Complementar el estudio enfocándose en la gestión del riesgo, tomando en cuenta la ISO/IEC 27005 Information Technology – Security techniques Information security risk management; debido a que esta investigación se enfocó más en la parte de análisis, permitiendo brindar nuevas salvaguardas y planes para mitigar, minimizar y/o evitar el riesgo de los activos de información.

- Realizar evaluaciones internas y externas para identificar brechas de seguridad con la finalidad de levantarlas y mejorar el sistema de seguridad de información.

VII. PROPUESTA: “Plan de seguridad de la información”

En este punto se describe algunos aspectos de un plan de seguridad de la información que será desarrollado para salvaguardar los activos de información.

7.1 Propósito

Finalizado el análisis de riesgos de los activos de información y obtenidas todas sus características (valor de activo, degradación, amenazas, vulnerabilidades impactos, riesgos y salvaguardas desplegadas), se conoce la situación actual de la organización en relación a la seguridad de sus activos de información, identificando varias vulnerabilidades respecto a la falta de políticas de seguridad de la información, al igual que varios controles de seguridad.

El paso siguiente según la Metodología MAGERIT (2012), que es la que se ha venido empleando en todo el desarrollo de investigación, indica que, posteriormente al análisis de riesgos se lleva acabo el tratamiento de los mismos, para lo que se es necesario realizar planes de seguridad. No obstante, el objetivo de esta propuesta es plasmar algunos proyectos de seguridad que conformen los controles basados en la norma ISO 27002:2013 la misma que consta de 14 dominios, 35 objetivos de control y 114 controles. No obstante, será de utilidad para el desarrollo del plan de seguridad de información que permita salvaguardar los activos de información, así pues, preparar a la organización para una futura certificación.

Para que el tratamiento de los riesgos sea eficaz, se necesita adoptar determinados controles y/o medidas de seguridad, que permitan, mitigar, reducir o eliminar el riesgo según sea el caso.

7.2 Ámbito

El plan de seguridad a desarrollar, permitirá definir proyectos de seguridad, los mismos que serán desarrollados a futuro, siendo aprobados por la dirección, se definirá cronogramas de implementación y costos de proyectos, adicionalmente en respuesta a las vulnerabilidades detalladas en el análisis de riesgos, se elaboró el manual de políticas de seguridad de la información, el mismo que aún no ha sido aprobado por la organización.

7.3 Referencias

Para el desarrollo del plan de seguridad se utilizó:

- Proyecto de análisis de riesgos de los activos de Información (Ver anexo N° 17)
- Metodología MAGERIT(2012)
- ISO/IEC 27002:2013

Además de esto, se tuvo en cuenta los trabajos previos brindados al inicio de la investigación.

7.4 Perspectivas del Plan de seguridad

El plan de seguridad nace como respuesta a las amenazas, vulnerabilidades y los niveles de riesgos identificados, para que la organización en estudio, tenga las herramientas necesarias para poder de alguna manera combatir con las amenazas detectadas y salvaguardas sus procesos que están conformados por los diferentes activos. La selección de los proyectos de seguridad se ha pensado para una futura certificación en seguridad de la información y asimismo, para salvaguardar los activos de información de las amenazas identificadas que suponen un nivel muy alto, y alto de riesgo.

A continuación se detallan las tareas que conforma el plan de seguridad.

- ✓ **PS1. Identificación de proyectos de seguridad:**

  En esta tarea se debe elaborar una serie de proyectos de seguridad, cuya planificación estará netamente relacionado con los resultados derivados del análisis de riesgos de los activos de información. Los ítems que se tomaran para cada uno de los proyectos, son los siguientes.

ID:	**Código del Proyecto**
Nombre Propuesta:	**Nombre de propuesta**
Tipo:	**En qué tipo es desarrollado (documento, prevención, procedimiento)**
Detalles	
Descripción del proyecto a realizar: **Salvaguardas y/o controles principales:** **Tareas:** **Beneficios:** **Responsable:**	
Dominio ISO	**Cuáles son los controles que se consideran ISO27002**
Activos del AARR	**Listado de activo al que afecta**

Amenazas Afrontadas	**Listado de amenazas que suponen un nivel muy alto y alto**
Tiempo estimado	**(Corto, medio o largo plazo).**
Estimación de Coste	
Presupuesto del costo económico. **Recurso:** **Dedicación:** **Coste Total:**	

- ✓ **PS2. Plan de ejecución**

  Se presentará un cronograma según costos y tiempo propuesto, así poder brindarle a la organización conocimiento de que proyectos son los que deben ejecutarse y cuando.

- ✓ **PS3. Ejecución**

  Este punto es a futuro, dependiendo de la organización. Ya que es aquí donde la empresa tiene que ver con las inversiones por proyectos y ver costo – beneficio.

VIII. REFERENCIAS

Aguilera, Lopez Purificacion. 2010. *Seguridad Informatica.* Madrid : Editex. S.A. págs. 23-240. ISBM: 978-84-9771-657-4.

Amutio, Gomez Miguel Angel y Hacienda, Ministerio de Hacienda y Administraciones Públicas. 2012. *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid : Ministerio de Hacienda y Administraciones Públicas.

Areitio, Javier. 2008. *Seguridad de la información. Redes, informática y sistemas de información.* Madrid : Paraninfo. pág. 566.

Correa, Garcia Carlos. 2009. La Seguridad de la Información. [En línea] . http://info-segur.blogspot.pe/.

Escrivá, Gascó Gema. 2013. *Seguridad Informatica.* Madrid : Macmillan Profesiona. pág. 216. 9788415656647.

INTECO, Instituto Nacional de Tecnologias de la Comunicaciones. *Implantación de un SGSI en la empresa.* España : s.n.

Mantilla , Blanco y Samuel, Alberto. 2003. *Internal control – Integrated Framework.* Bogotá : s.n.

Merino, Bada Cristina y Cañizares Sales, Ricardo. 2011. *Implantación de un sistema de gestión de seguridad de la información según ISO 2700.* Madrid : s.n. pág. 292. ISBN-13:978-84-92735-87-7.

PriteshGupta.com. 2012. ISO27002:2013. *Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002.*

Ramos, Gonzales Miguel A. y Del Peso Navarro, Emilio. 2002. *La seguridad de los datos de caracter personal.* s.l. : Diaz Santos, pág. 287. ISBN: 978-84-7975-527-7.

Segunda Cohorte, Doctorado. 2014. *Seguridad de la Informacion.* Guatemala : s.n.

Tejada, Ester Chicano. 2015. *Auditoría de seguridad informática. IFCT0109.* s.l. : IC Editorial.

ANEXOS

Anexo N° 01: Validación de Instrumentos

UNIVERSIDAD CESAR VALLEJO FILIAL PIURA
ESCUELA DE INGENIERIA DE SISTEMAS

FICHA DE VALIDACIÓN DE INSTRUMENTOS

1. **INFORMACIÓN DEL EXPERTO:**
   - **1.1** Nombre y Apellido : JORGE LUIS ALVARADO PAUTA
   - **1.2** Profesión : ING. INFORMATICO
   - **1.3** Grados académicos : INGENIERO
   - **1.4** Institución donde trabaja : Universidad Cesar Vallejo filial Piura
   - **1.5** Cargo que desempeña : DOCENTE TP - AUDITORIA Y SEG. INF.
   - **1.6** Teléfono : 969189977
   - **1.7** Correo electrónico : jorge.alvarado@cip.org.pe

2. **NOMBRE DEL INVESTIGADOR:** Valdiviezo Mogollón, Yesenia Stephanie

3. **SOBRE LA INVESTIGACIÓN:**

   3.1 Título de la investigación:
   "Análisis de Riesgos de la información de la Clínica Internacional – Sede Piura haciendo uso de la metodología MAGERIT"

   3.2 Objetivo de estudio:
   Objetivo general:
   Analizar los riesgos de los activos de información identificados en la Clínica Internacional Sede – Piura haciendo uso de la metodología MAGERIT.

   3.3 Campo o Variable que se pretende medir:
   Análisis de riesgo de la información

   3.4. Dimensiones de la variable
   - Activos
   - Amenazas
   - Vulnerabilidades
   - Salvaguardas

   3.5. Instrumentos Elaborados
   - Ficha de Registro N°1: Identificación de Activos
   - Ficha de Registro N°2: Valoración de Activos
   - Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos
   - Ficha de Registro N°4: Valoración De Amenazas
   - Ficha de Registro N°5: Determinación de Impacto
   - Ficha de Registro N°6: Valoración de Vulnerabilidades
   - Ficha de Registro N°7: Estimación de Riesgo
   - Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual

4. **APRECIACIONES:**

4.1 Pertinencia de los ítems con los objetivos:

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE	OBSERVACIONES
Ficha de Registro N°1: Identificación de Activos	✓			
Ficha de Registro N°2: Valoración de Activos	✓			
Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos	✓			
Ficha de Registro N°4: Valoración De Amenazas	✓			
Ficha de Registro N°5: Determinación de Impacto	✓			
Ficha de Registro N°6: Valoración de Vulnerabilidades	✓			
Ficha de Registro N°7: Estimación de Riesgo	✓			
Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual	✓			

4.2 Pertinencia de los ítems con las variables/indicadores:

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE	OBSERVACIONES
Ficha de Registro N°1: Identificación de Activos	✓			
Ficha de Registro N°2: Valoración de Activos	✓			
Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos	✓			
Ficha de Registro N°4: Valoración De Amenazas	✓			
Ficha de Registro N°5: Determinación de Impacto	✓			
Ficha de Registro N°6: Valoración de Vulnerabilidades	✓			
Ficha de Registro N°7: Estimación de Riesgo	✓			
Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual	✓			

4.3 Pertinencia de los ítems con las dimensiones-Organizadores

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE	OBSERVACIONES
Ficha de Registro N°1: Identificación de Activos	✓			
Ficha de Registro N°2: Valoración de Activos	✓			
Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos	✓			
Ficha de Registro N°4: Valoración De Amenazas	✓			
Ficha de Registro N°5: Determinación de Impacto Ficha de Registro N°6: Valoración de Vulnerabilidades	✓			
Ficha de Registro N°7: Estimación de Riesgo	✓			
Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual	✓			

4.4 Pertinencia de los ítems con los indicadores:

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE	OBSERVACIONES
Ficha de Registro N°1: Identificación de Activos	✓			
Ficha de Registro N°2: Valoración de Activos	✓			
Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos	✓			
Ficha de Registro N°4: Valoración De Amenazas	✓			
Ficha de Registro N°5: Determinación de Impacto	✓			
Ficha de Registro N°6: Valoración de Vulnerabilidades	✓			
Ficha de Registro N°7: Estimación de Riesgo	✓			
Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual	✓			

4.5 Redacción de los ítems

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE	OBSERVACIONES
Ficha de Registro N°1: Identificación de Activos	✓			
Ficha de Registro N°2: Valoración de Activos	✓			
Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos	✓			
Ficha de Registro N°4: Valoración De Amenazas	✓			
Ficha de Registro N°5: Determinación de Impacto	✓			
Ficha de Registro N°6: Valoración de Vulnerabilidades	✓			
Ficha de Registro N°7: Estimación de Riesgo	✓			
Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual	✓			

5. CONCLUSIONES: LOS INSTRUMENTOS VALIDADOS, SON RAZONABLEMENTE SUFICIENTES, PARA LA CONSECUSIÓN DE LOS OBJETIVOS PROPUESTOS.

NOMBRE JORGE LUIS ALVARADO PAUTA

FIRMA

Piura, 2015

JORGE LUIS ALVARADO PAUTA
INGENIERO INFORMATICO
Reg. CIP N° 121486

UNIVERSIDAD CESAR VALLEJO FILIAL PIURA
ESCUELA DE INGENIERIA DE SISTEMAS

FICHA DE VALIDACIÓN DE INSTRUMENTOS

1. **INFORMACIÓN DEL EXPERTO:**
   - **1.1** Nombre y Apellido : Anthony Paul Tavara Ramos
   - **1.2** Profesión : Ing. Informatico
   - **1.3** Grados académicos : M. Sc Ing. Informatico
   - **1.4** Institución donde trabaja : Universidad Cesar Vallejo filial Piura
   - **1.5** Cargo que desempeña : Docente
   - **1.6** Teléfono : 979188720
   - **1.7** Correo electrónico : anthony_tavara@yahoo.com

2. **NOMBRE DEL INVESTIGADOR:** Valdiviezo Mogollón, Yesenia Stephanie

3. **SOBRE LA INVESTIGACIÓN:**

3.1 Título de la investigación:

"Análisis de Riesgos de la información de la Clínica Internacional – Sede Piura haciendo uso de la metodología MAGERIT"

3.2 Objetivo de estudio:

Objetivo general:

Analizar los riesgos de los activos de información identificados en la Clínica Internacional Sede – Piura haciendo uso de la metodología MAGERIT.

3.3 Campo o Variable que se pretende medir:

Análisis de riesgo de la información

3.4. Dimensiones de la variable

- Activos
- Amenazas
- Vulnerabilidades
- Salvaguardas

3.5. Instrumentos Elaborados

- Ficha de Registro N°1: Identificación de Activos
- Ficha de Registro N°2: Valoración de Activos
- Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos
- Ficha de Registro N°4: Valoración De Amenazas
- Ficha de Registro N°5: Determinación de Impacto
- Ficha de Registro N°6: Valoración de Vulnerabilidades
- Ficha de Registro N°7: Estimación de Riesgo
- Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual

4. **APRECIACIONES:**

4.1 Pertinencia de los ítems con los objetivos:

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE	OBSERVACIONES
Ficha de Registro N°1: Identificación de Activos	✓			
Ficha de Registro N°2: Valoración de Activos	✓			
Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos	✓			
Ficha de Registro N°4: Valoración De Amenazas	✓			
Ficha de Registro N°5: Determinación de Impacto	✓			
Ficha de Registro N°6: Valoración de Vulnerabilidades		✓		Rango valoración de vulnerabilidades no por tiempo.
Ficha de Registro N°7: Estimación de Riesgo	✓			
Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual	✓			

4.2 Pertinencia de los ítems con las variables/indicadores:

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE	OBSERVACIONES
Ficha de Registro N°1: Identificación de Activos	✓			
Ficha de Registro N°2: Valoración de Activos	✓			
Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos	✓			
Ficha de Registro N°4: Valoración De Amenazas	✓			
Ficha de Registro N°5: Determinación de Impacto	✓			
Ficha de Registro N°6: Valoración de Vulnerabilidades	✓			
Ficha de Registro N°7: Estimación de Riesgo	✓			
Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual	✓			

4.3 Pertinencia de los ítems con las dimensiones-Organizadores

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE	OBSERVACIONES
Ficha de Registro N°1: Identificación de Activos	✓			
Ficha de Registro N°2: Valoración de Activos	✓			
Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos	✓			
Ficha de Registro N°4: Valoración De Amenazas	✓			
Ficha de Registro N°5: Determinación de Impacto Ficha de Registro N°6: Valoración de Vulnerabilidades	✓ ✓			
Ficha de Registro N°7: Estimación de Riesgo	✓			
Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual	✓			

4.4 Pertinencia de los ítems con los indicadores:

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE	OBSERVACIONES
Ficha de Registro N°1: Identificación de Activos	✓			
Ficha de Registro N°2: Valoración de Activos	✓			
Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos	✓			
Ficha de Registro N°4: Valoración De Amenazas	✓			
Ficha de Registro N°5: Determinación de Impacto	✓			
Ficha de Registro N°6: Valoración de Vulnerabilidades		✓		Revisar valoración
Ficha de Registro N°7: Estimación de Riesgo	✓			
Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual	✓			

4.5 Redacción de los ítems

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE	OBSERVACIONES
Ficha de Registro N°1: Identificación de Activos	✓			
Ficha de Registro N°2: Valoración de Activos	✓			
Ficha de Registro N°3: Identificación De Amenazas Asociadas A Los Activos	✓			
Ficha de Registro N°4: Valoración De Amenazas	✓			
Ficha de Registro N°5: Determinación de Impacto	✓			
Ficha de Registro N°6: Valoración de Vulnerabilidades	✓			
Ficha de Registro N°7: Estimación de Riesgo	✓			
Ficha de Registro N°8: Identificación y Valoración de Salvaguardas y Riesgo residual	✓			

5. CONCLUSIONES:
Instrumentos debidamente validados y de aplicación para la investigación

NOMBRE Anthony Paul Tavara Rosas

FIRMA

Piura, 2015

Anexo N° 10: Constancia de realización de estudio.

Clínica Internacional
Nuestros pacientes primero

CONSTANCIA

En mi calidad de Sub Gerente Administrativo de la **"Clínica Internacional – Sede Piura"**, hago constar que **Yesenia Stephanie Valdiviezo Mogollón**, estudiante de Ingeniería de Sistemas de la Universidad César Vallejo – Piura, identificada con **DNI 46764883**, quien se desempeña como practicante en el área de operaciones realizó una investigación en la Institución que represento, como parte de la elaboración del proyecto y desarrollo de su Tesis.

Asimismo, la alumna elaboró una propuesta para mejorar los resultados obtenidos, la cual corresponde a un plan de seguridad aplicable a la institución.

Cabe resaltar que a la alumna se le brindaron las facilidades correspondientes para que la investigación continúe su curso de la mejor manera, proporcionando la información adecuada y necesaria.

Sin otro particular, pongo a disposición el presente documento para los fines que se crean convenientes.

Piura, 15 de Junio del 2016

Atentamente,

Luis Torres Núñez
SUB GERENTE ADMINISTRATIVO
CLINICA INTERNACIONAL S.A.

Anexo N° 03: Instrumento Identificación de Activos

IDENTIFICACION DE ACTIVOS		
NOMBRE:		
PUESTO:		
¿Qué activos son escenciales para que Ud. Consiga sus objetivos?		
ACTIVOS POR TIPO		(X) Si
D	Datos/Información	
[files]	Ficheros	
[backup]	Copias de respaldo	
[conf]	Datos de configuración	
[int]	Datos de gestion interna	
[password]	Crdenciales (contraseñas)	
[auth]	Datos de validacion de Credenciales	
[acl]	Datos de control de acceso	
[log]	Registro de actividad	
[source]	Codigo fuente	
[exe]	Codigo ejecutable	
[test]	Datos de prueba	
S	Servicios	
[anon]	Anónimo (sin requerir identificación del usuario)	
[pub]	Al público en general (sin relación contractual)	
[ext]	A usuarios externos (bajo una relación contractual)	
[int]	Interno (usuarios y medios de la propia organización)	
[cont]	Contratado a terceros (se presta con medios ajenos)	
[www]	World wide web	
[telnet]	Acceso remoto a cuenta local	
[email]	Correo electrónico	
[voip]	Voz sobre ip	
[file]	Almacenamiento de ficheros	
[print]	Servicio de impresión	
[ftp]	Transferencia de ficheros	
[s.back]	servicio de copias de respaldo (backup)	
[edi]	Intercambio electrónico de datos	
[dir]	Servicio de directorio	
[dns]	Servidor de nombres de dominio	
[idm]	Gestión de identidades	
[ipm]	Gestión de privilegios	
[crypto]	Servicios criptográficos	
[key_gen]	Generación de claves	
[integrity]	Protección de la integridad	
[encryption]	Cifrado	
[auth]	Autenticación	
[sign]	Firma electrónica	
[time]	Fechado electrónico	
[crypto. o]	Otros....	
[pki]	Pki - infraestructura de clave pública	
[ra]	Autoridad de registro	
[ba]	Autoridad de validación	
[tsa]	Autoridad de fechado electrónico	
[aa]	Autoridad de atributos	
[pki. o]	Otros...	

SW	Aplicaciones/Software
[prp]	Desarrollo propio (in house)
[sub]	Desarrollo a medida (subcontratado)
[browser]	Navegador web
[Serv.p]	Servidor de presentación
[app]	Servidor de aplicaciones
[email_client]	Cliente de correo electrónico
[email_server]	Servidor de correo electrónico
[directory]	Servidor de directorio
[s.file]	Servidor de ficheros
[dbms]	Sistema de gestión de bases de datos
[tm]	Monitor transaccional
[office]	Ofimática
[av]	Anti virus
[os]	Sistema operativo
[windows]	Windows
[solaris]	Solaris
[linux]	Linux
[os.o]	Otros...
[ts]	Servidor de terminales
[a.back]	Sistema de backup

HW	Equipos Informáticos
[host]	Grandes equipos (host)
[mid]	Equipos medios
[pc]	Informática personal
[vhost]	Equipos virtuales
[cluster]	Cluster
[mobile]	Informática móvil
[pda]	Agendas electrónicas
[easy]	Fácilmente reemplazable
[data]	Que almacena datos
[peripheral]	Periféricos
[print]	Medios de impresión
[scan]	Escáner
[crypto]	Dispositivo criptográfico
[peripheral.o]	Otros...
[df]	Dispositivo de frontera
[network]	Soporte de la red
[modem]	Módem
[hub]	Concentrador
[switch]	Conmutador
[router]	Encaminador
[bridge]	Puente
[gtwy]	Pasarela
[network.o]	Otros...
[firewall]	Cortafuegos
[wap]	Punto de acceso inalambrico
[pabx]	Centralita telefónica
[ipphone]	Teléfono IP

SI	Soportes de Información
[electronic]	Electrónicos
[disk]	Discos
[vdisk]	Discos virtuales
[san]	Almacenamiento en red
[disquette]	Disquetes
[cd]	Cederrón (cd-rom)
[usb]	Dispositivos usb
[dvd]	Dvd
[tape]	Cinta magnética
[mc]	Tarjetas de memoria
[ic]	Tarjetas inteligentes
[electronic.o]	Otros...
[non_electronic]	No electrónicos
[printed]	Material impreso
[tape]	Cinta de papel
[film]	Microfilm
[cards]	Tarjetas perforadas
[non_electronic.o]	Otros

AUX	Equipamiento Auxiliar
[power]	Fuentes de alimentación
[ups]	Sai - sistemas de alimentación ininterrumpida
[gen]	Generadores eléctricos
[ac]	Equipos de climatización
[cabling]	Cableado
[wire]	Cable eléctrico
[fiber]	Fibra óptica
[robot]	Robots
[tape]	... De cintas
[disk]	... De discos
[supply]	Suministros esenciales
[destroy]	Equipos de destrucción de soportes de información
[furniture]	Mobiliario: armarios, etc
[safe]	Cajas Fuertes

COM	Redes de Comunicaciones
[PSTN]	Red telefónica
[ISDN]	RDSI (red digital)
[X25]	X25 (red de datos)
[ADSL]	Adsl
[pp]	Punto a punto
[radio	Red inalámbrica
[wifi]	Wifi
[mobile]	Telefonía movil
[sat]	Por satélite
[LAN]	Red local
[VLAN]	LAN virtual
[MAN]	Red metropolitana
WAN]	Red de área amplia
[Internet]	Internet
[vpn]	Red privada virtual

L	Instalaciones
[site]	Emplazamiento
[building]	Edificio
[local]	Local
[mobile]	Plataformas móviles
[car]	Vehículo terrestre: coche, camión, etc.
[ship]	Vehículo marítimo: buque, lancha, etc.
[plane]	Vehículo aéreo: avión, etc.
[shelter]	Contenedores
[channel]	Canalización

P	Personal
[ue]	Usuarios externos
[ui]	Usuarios internos
[op]	Operadores
[adm]	Administradores de sistemas
[com]	Administradores de comunicaciones
[dba]	Administradores de BBDD
[sec]	Administradores de seguridad
[des]	Desarrolladores/programadores
[sub]	Subcontratas
[prov]	Proveedores

Listar si existen mas activos que tenga que proteger que no esten en el listado	
Cod	Nombre del activo

Anexo N° 04: Valoración de activos

FICHA DE REGISTRO N°2		
VALORACION DE ACTIVOS		
Instrucciones: Se presentan los aspecto que se deben considerar para la valoración de los activos presentes en la Organización , atendiendo a las dimensiones principales de la información:		
Confidencialidad [C] ¿qué daño causaría que el activo lo conociera quien no debe?		
Integridad [I] ¿qué perjuicio causaría que el activo estuviera dañado o corrupto?		
Disponibilidad [D] ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?		
Escala	**Descripción**	**V**
MB = Muy Bajo	Irrelevante a efectos prácticos	1
B = Bajo	Daño menor	2
M = Medio	Daño Importante	3
A = Alto	Daño grave	4
MA = Muy Alto	Daño muy grave	5
2	De bajo interés para la competencia Pudiera causar una pérdida menor de la confianza dentro de la Organización	
3	Probablemente cause la interrupción de actividades propias de la Organización Probablemente impediría la operación efectiva de una parte de la Organización Probablemente afecte negativamente a las relaciones internas de la Organización	
4	Probablemente afecte gravemente a un grupo de individuos Alto interés para la competencia Probablemente perjudique la eficacia o seguridad de la misión operativa o logística	
5	Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal Causa de pérdidas económicas excepcionalmente elevadas Probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre	

NOMBRE:

¿De qué manera la perdida del activo afecta la C.I.D.?				
ACTIVOS POR TIPO		Dimensiones		
		C	I	D
D	**Datos/Información**			
[bd.1]	Base de Datos Atenciones			
[bd.2]	Base de Datos General			
[bd.3]	Base de Datos Myzro			
[bd.4]	Base de Datos Kardex			
[exe]	Codigo ejecutable			
[source.1]	Codigo Fuente Atenciones			
[source.2]	Codigo Fuente Myzro			
[source.3]	Codigo Fuente Ventas			
[backup]	Copias de respaldo			
[password]	Crdenciales (contraseñas)			
[conf]	Datos de configuración			
[acl]	Datos de control de acceso			
[test]	Datos de prueba			
[files]	Ficheros			
[hc]	Historias Clinicas			

S	Servicios			
[file]	Almacenamiento de ficheros			
[email]	Correo electrónico Institucional			
[www]	Internet			
[cont]	Proveedores de T.I			
[s.back]	servicio de copias de respaldo (backup)			
[print]	Servicio de impresión			
[sst]	Servicio de Soporte Técnico Interno			
[dns]	Servidor de nombres de dominio			
[voip]	Telefonía IP			

SW	Aplicaciones/Software			
[browser.1]	Google Chrome			
[browser.2]	Internet Explorer			
[av]	Mcafee			
[office]	Microsof Office			
[dbms.1]	MySQL			
[dbms.2]	Oracle			
[prp.1]	Sistema Atenciones			
[a.back]	Sistema de backup			
[prp.2]	Sistema Myzro			
[prp.3]	Sistema Kairos			
[prp.4]	Sistemas General			
[dbms.3]	SQL Server 2008			
[dbms.4]	Visual Fox Pro			
[windows.1]	Windows 7			
[windows.2]	Windows XP			

HW	Equipos Informáticos			
[print.1]	Impresora Láser			
[print.2]	Impresora Matricial			
[pc.1]	PC Administrativos General			
[pc.2]	PC Clinica			
[pc.3]	PC Gerencia Administrativa			
[pc.4]	PC Informática			
[pc.5]	PC Jefaturas			
[scan]	Scanner			
[pabx]	Servidor Central Telefónica			
[servi.1]	Servidor de Backups			
[servi.2]	Servidor Myzro			
[switch]	Switches			

SI	Soportes de Información			
[san]	Almacenamiento en red			
[cca]	Contratos, convenios, y acuerdos			
[printed.1]	Diccionario de Datos			
[disk.2]	Disco Externo			
[printed.2]	Documentacion de los Sistemas			
[printed.3]	Informes de Auditoria Médica			
[usb]	USB Administrativos General			

AUX	Equipamiento Auxiliar			
[ac]	Aires acondicionados			
[power]	Fuentes de alimentación			
[gen]	Generadores eléctricos			
[prp.5]	Sistema de control biometrico dactilar y facial			
[furniture.1]	Stand Madera Oficinas			
[furniture.2]	Stand Metálica Oficinas			
[ups]	UPS Informática			

COM	Redes de Comunicaciones			
[WAN]	Red de área amplia			
[LAN]	Red local			
[PSTN]	Red telefónica			
[wifi]	Wifi			

L	Instalaciones			
[building.1]	Edificio Clinica			
[building.2]	Edificio Torre Nueva			
[local.1]	Oficinas 1 piso			
[local.2]	Oficinas 2 piso			
[local.3]	Oficinas 3 piso			
[local.4]	Sector Consultorios Medicos Clinica			
[local.5]	Sector Consultorios Medicos Torre Nueva			
[local.6]	Sector Historias Clinicas			
[local.7]	Sector Informatica			

P	Personal			
[ui.1]	Administrativos General			
[ui.2]	Gerencia Administrativa			
[ui.3]	Jefaturas			
[adm]	Administradores de sistemas			
[des]	Desarrolladores/programadores			
[ui.4]	Personal Asistencial, Ténicos y Laboratoristas			
[ui.5]	Personal de Auditoria Medica			
[ui.6]	Personal Hist Clinicas			

Anexo N° 05: Instrumento identificación de amenazas

FICHA DE REGISTRO N°3 IDENTIFICACION DE AMENAZAS		
Instrucciones: Se presentan los aspecto que se deben considerar para la valoracion de la degradacion del activo y la probabilidad de ocurrencia, teniendo en cuenta:		
¿Qué amenazas identifica que oueden afectar a sus activos son escenciale?		
AMENAZAS		(X) Si
N	Amenazas Naturales	
[N.1]	Daños por fuego	
[N.2]	Daños por agua	
[N.3]	Desastres Naturales	
I	Origen Industrial	
[I.1]	Daños por fuego	
[I.2]	Daños por agua	
[I.3]	Desastres Industriales	
[I.4]	Contaminación mecánica	
[I.5]	Contaminación electromagnetica	
[I.6]	Averías de origen físico o lógico	
[I.7]	Corte de suministro eléctrico	
[I.8]	Condiciones inadecuadas de temperatura o humedad	
[I.9]	Falla de servicios de comunicaciones	
[I.10]	Interrupción de otros servicios y suministros esenciales	
[I.11]	Degradación de los soportes de almacenamiento de la información	
[I.12]	Emanaciones electromagnéticas	
E	Errores y fallos no intencionados	
[E.1]	Errores de usuarios	
[E.2]	Errores de administrador	
[E.3]	Errores de Monitorización	
[E.4]	Errores de Configuración	
[E.5]	Deficiencias de la organización	
[E.6]	Disfusión de software dañino	
[E.7]	Errores de reencaminamiento	
[E.8]	Errores de secuencia	
[E.9]	Escapes de información	
[E.10]	Alteración accidental de información	
[E.11]	Destruccion de información	
[E.12]	Fugas de información	
[E.13]	Vulnerabilidad de los programas(software)	
[E.14]	Errores en mantenimiento / Actualizacion de software	
[E.15]	Errores en mantenimiento / Actualizacion de equipos	
[E.16]	Caida de sistema por agotamiento de recursos.	
[E.17]	Pérdida de equipos	
[E.18]	Indisponibilidad del personal	

A	Ataques intencionados
[A.1]	Manipulación de los registros de actividad (log)
[A.2]	Manipulación de la configuración
[A.3]	Suplantación de identidad
[A.4]	Abuso de privilegios de acceso
[A.5]	Uso no previsto
[A.6]	Difusión de software dañino
[A.7]	Acceso no autorizado
[A.8]	Repudio
[A.9]	Intercepción de información
[A.10]	Modificación deliberada de información
[A.11]	Destrucción de información
[A.12]	Divulgación de información
[A.13]	Manipulacion de Programas
[A.14]	Manipulacion de Equipos
[A.15]	Denegacion de Servicio
[A.16]	Robo
[A.17]	Ataque destructivo
[A.18]	Ocupación enemiga
[A.19]	Indisponibilidad del personal
[A.20]	Extorsion
[A.21]	Ingenieria social

Listar si existen mas amenazas que no esten en el lisytado	
Cod	Nombre del activo

Anexo N° 06: Instrumento identificación y valoración de salvaguarda.

FICHA DE REGISTRO N°4		
VALORACION DE SALVAGUARDAS		
Instrucciones: Se presentan los aspecto que se deben considerar para la determinación de las salvaguardas, atendiendo a las dimensiones principales de la información: **Eficiencia [E]**		
Escala	**V**	**V**
L5 = Optimizado	**100%**	Mejora continua
L4 =Gestionado y Medible	**90%**	Monitorizado
L3 = Procesado y medible	**70%**	En Funcionamiento
L2 = Reproducible, pero intuitivo	**40%**	Parcialmente realizado
L1 = Inicial/ ad hoc	**10%**	iniciado
L0 = Inexistente	**0%**	Inexistente

SALVAGUARDAS	(X) Si	% E
Protecciones generales u horizontales		
Identificación y autenticación		
Control de acceso lógico		
Segregación de tareas		
Gestión de incidencias		
Herramientas de seguridad		
Herramienta contra código dañino		
IDS/IPS: Herramienta de detección / prevención de intrusión		
Herramienta de chequeo de configuración		
Herramienta de análisis de vulnerabilidades		
Herramienta de monitorización de tráfico		
DLP: Herramienta de monitorización de contenidos		
Herramienta para análisis de logs		
Verificación de las funciones de seguridad		
Gestión de vulnerabilidades		
Registro y auditoría		
Protección de la Información		
Copias de seguridad de los datos (backup)		
Aseguramiento de la integridad		
Cifrado de la información		
Uso de firmas electrónicas		
Uso de servicios de fechado electrónico (time stamping)		

Protección de los Servicios		
Aseguramiento de la disponibilidad		
Aceptación y puesta en operación		
Se aplican perfiles de seguridad		
Explotación		
Gestión de cambios (mejoras y sustituciones)		
Terminación		
Protección de servicios y aplicaciones web		
Protección del correo electrónico		
Protección del directorio		
Protección del servidor de nombres de dominio (DNS)		
Teletrabajo		
Voz sobre IP		
Protección de las aplicaciones (software)		
Protección de las Aplicaciones Informáticas		
Copias de seguridad (backup)		
Puesta en producción		
Se aplican perfiles de seguridad		
Explotación / Producción		
Cambios (actualizaciones y mantenimiento)		
Terminación		

Protección de los equipos (hardware)		
Protección de los Equipos Informáticos		
Puesta en producción		
Se aplican perfiles de seguridad		
Aseguramiento de la disponibilidad		
Operación		
Cambios (actualizaciones y mantenimiento)		
Terminación		
Informática móvil		
Reproducción de documentos		
Protección de la centralita telefónica (PABX)		
Protección de las comunicaciones		
Protección de las Comunicaciones		
Entrada en servicio		
Se aplican perfiles de seguridad		
Aseguramiento de la disponibilidad		
Autenticación del canal		
Protección de la integridad de los datos intercambiados		
Protección criptográfica de la confidencialidad de los datos interc		
Operación		
Cambios (actualizaciones y mantenimiento)		
Terminación		
Internet: uso de ? acceso a		
Seguridad Wireless (WiFi)		
Telefonía móvil		
Segregación de las redes en dominios		

Protección en los puntos de interconexión con otros sistemas		
Puntos de interconexión: conexiones entre zonas de confianza		
Sistema de protección perimetral		
Protección de los equipos de frontera		
Protección de los soportes de información		
Protección de los Soportes de Información		
Aseguramiento de la disponibilidad		
Protección criptográfica del contenido		
Limpieza de contenidos		
Destrucción de soportes		
Elementos Auxiliares		
Aseguramiento de la disponibilidad		
Instalación		
Suministro eléctrico		
Climatización		
Protección del cableado		
Seguridad física – Protección de las instalaciones		
Protección de las Instalaciones		
Diseño		
Defensa en profundidad		
Control de los accesos físicos		
Aseguramiento de la disponibilidad		
Terminación		
relativas al personal		
Gestión del Personal		
Formación y concienciación		
Aseguramiento de la disponibilidad		
Tipo organizativo		
Organización		
Gestión de riesgos		
Planificación de la seguridad		
Inspecciones de seguridad		
Continuidad de operaciones		
Continuidad del negocio		
Análisis de impacto (BIA)		
Plan de Recuperación de Desastres (DRP)		
Externalización		
Relaciones Externas		
Acuerdos para intercambio de información y software		
Acceso externo		
Servicios proporcionados por otras organizaciones		
Personal subcontratado		
Adquisición y desarrollo		
Adquisición / desarrollo		
Servicios: Adquisición o desarrollo		
Aplicaciones: Adquisición o desarrollo		
Equipos: Adquisición o desarrollo		
Comunicaciones: Adquisición o contratación		
Soportes de Información: Adquisición		
Productos certificados o acreditados		

Anexo N° 07: Matriz de Identificación de activos

IDENTIFICACION DE ACTIVOS POR PERSONAL INVOLUCRADO		Comité de Analisis de Riesgos															
		GA	SJ	JA	JR	JAT	JSAC	JC	JF	JFR	JO	JM	JHC	JS	JSAC	JAUD	GM	JIT
		Gerente Adm	Secretaria Jef.	Jefa de Adm	Jefa RRHH	Jefa Asistencial	Jefa Cobranzas	Jefa Contabilidad	Jefa Facturación	Jefa Farmacia	Jefa Operaciones	Jefe Mantenimiento	Jefe HC	Jefa de Servicios	Jefa de SAC	Jefa de Aud. Med	Gerente Med.	Jefe Sistemas
D	**Datos/Información**																	
[files]	Ficheros																	x
[backup]	Copias de respaldo																	x
[conf]	Datos de configuración																	x
[int]	Datos de gestion interna																	
[password]	Crdenciales (contraseñas)																	x
[auth]	Datos de validacion de Credenciales																	
[acl]	Datos de control de acceso																	x
[log]	Registro de actividad																	
[source]	Codigo fuente																	x
[exe]	Codigo ejecutable																	x
[test]	Datos de prueba																	x
S	**Servicios**																	
[anon]	Anónimo (sin requerir identificación del usuario)																	
[pub]	Al público en general (sin relación contractual)																	
[voip]	Voz sobre ip																	x
[app]	Servidor de aplicaciones																	
[email_client]	Cliente de correo electrónico																	
[email_server]	Servidor de correo electrónico																	
[directory]	Servidor de directorio																	
[s.file]	Servidor de ficheros																	
[dbms]	Sistema de gestión de bases de datos																	x
[tm]	Monitor transaccional																	
[office]	Ofimática	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[av]	Anti virus	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[os]	Sistema operativo																	
[windows]	Windows	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[solaris]	Solaris																	
[linux]	Linux																	
[os.o]	Otros...																	
[ts]	Servidor de terminales																	
[a.back]	Sistema de backup																	x

HW	Equipos Informáticos																
[host]	Grandes equipos (host)																
[mid]	Equipos medios																
[pc]	Informática personal	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[vhost]	Equipos virtuales																
[cluster]	Cluster																
[mobile]	Informática móvil																
[pda]	Agendas electrónicas																
[easy]	Fácilmente reemplazable																
[data]	Que almacena datos	x		x												x	x
[peripheral]	Periféricos																
[print]	Medios de impresión	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[scan]	Escáner	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[crypto]	Dispositivo criptográfico																
[peripheral.o]	Otros...																
[df]	Dispositivo de frontera																
[network]	Soporte de la red																
[modem]	Módem																
[hub]	Concentrador																
[switch]	Conmutador																x
[router]	Encaminador																
[bridge]	Puente																
[gtwy]	Pasarela																
[network.o]	Otros...																
[firewall]	Cortafuegos																x
[wap]	Punto de acceso inalambrico																
[pabx]	Centralita telefónica	x	x											x			x
[ipphone]	Teléfono IP																x

SI	Soportes de Información																
[electronic]	Electrónicos																
[disk]	Discos	x															x
[vdisk]	Discos virtuales																
[san]	Almacenamiento en red																x
[disquette]	Disquetes																
[cd]	Cederrón (cd-rom)																
[usb]	Dispositivos usb		x	x										x			x
[dvd]	Dvd																
[tape]	Cinta magnética																
[mc]	Tarjetas de memoria																
[ic]	Tarjetas inteligentes																
[electronic.o]	Otros...																
[non_electronic]	No electrónicos																
[printed]	Material impreso																x
[tape]	Cinta de papel																
[film]	Microfilm																
[cards]	Tarjetas perforadas																
[non_electronic.o]	Otros																

AUX	Equipamiento Auxiliar																
[power]	Fuentes de alimentación																x
[ups]	Sai - sistemas de alimentación ininterrumpida																x
[gen]	Generadores eléctricos																x
[ac]	Equipos de climatización																x
[cabling]	Cableado																
[wire]	Cable eléctrico																
[fiber]	Fibra óptica																
[robot]	Robots																
[tape]	... De cintas																
[disk]	... De discos																
[supply]	Suministros esenciales																
[destroy]	Equipos de destrucción de soportes de información																
[furniture]	Mobiliario: armarios, etc	x															x
[safe]	Cajas Fuertes																

COM	Redes de Comunicaciones																
[PSTN]	Red telefónica																x
[ISDN]	RDSI (red digital)																
[X25]	X25 (red de datos)																
[ADSL]	Adsl																
[pp]	Punto a punto																
[radio	Red inalámbrica	x															
[wifi]	Wifi																x
[mobile]	Telefonía movil																
[sat]	Por satélite																
[LAN]	Red local																x
[VLAN]	LAN virtual																
[MAN]	Red metropolitana																
WAN]	Red de área amplia																x
[Internet]	Internet																x
[vpn]	Red privada virtual																

L	Instalaciones																
[site]	Emplazamiento																
[building]	Edificio	x															x
[local]	Local																x
[mobile]	Plataformas móviles																
[car]	Vehículo terrestre: coche, camión, etc.																
[ship]	Vehículo marítimo: buque, lancha, etc.																
[plane]	Vehículo aéreo: avión, etc.																
[shelter]	Contenedores																
[channel]	Canalización																

P	Personal																
[ue]	Usuarios externos																
[ui]	Usuarios internos	x															x
[op]	Operadores	x															
[adm]	Administradores de sistemas	x															x
[com]	Administradores de comunicaciones																
[dba]	Administradores de BBDD																
[sec]	Administradores de seguridad																
[des]	Desarrolladores/programadores	x															x
[sub]	Subcontratas																
[prov]	Proveedores	x															

Otros	Adicionales																
[Hist]	Historias Clinicas											x					x
[bd]	Base de Datos																
[sst]	Servicio de Soporte Técnico Interno																x
[sst]	Contratos, convenios, y acuerdos																x

Anexo N° 08: Matriz de valoración de activos

VALORACION DE ACTIVOS POR PERSONAL INVOLUCRADO CON EL ACTIVO

CONFIDENCIALIDAD

Código	Activo	GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
D	Datos/Información																					
[bd.1]	Base de Datos Atenciones																	5	5	5	5	5
[bd.2]	Base de Datos General																	4	4	4	5	4
[bd.3]	Base de Datos Myzro																	4	5	5	5	5
[bd.4]	Base de Datos Kardex																	5	4	5	5	5
[exe]	Codigo ejecutable																	5	5	4	5	5
[source.1]	Codigo Fuente Atenciones																	4	4	3	4	4
[source.2]	Codigo Fuente Myzro																	5	5	5	5	5
[source.3]	Codigo Fuente Ventas																	5	4	5	5	5
[backup]	Copias de respaldo																	5	5	4	5	5
[password]	Crdenciales (contraseñas)																	3	3	4	4	3
[conf]	Datos de configuración																	4	4	3	4	4
[acl]	Datos de control de acceso																	5	4	5	5	5
[test]	Datos de prueba																	3	4	3	3	3
[files]	Ficheros																	4	3	4	4	4
[hc]	Historias Clinicas												5					4	5	5	5	5
S	Servicios																					
[file]	Almacenamiento de ficheros																	5	5	4	5	5
[email]	Correo electrónico Institucion	5	5	5	4	4	4	4	5	4	5	4	4	4	4	5	5	4	5	5	5	5
[www]	Internet	5	5	5	4	4	5	5	5	5	4	5	5	4	5	4	3	4	4	5	5	5
[cont]	Proveedores de T.I	5		5	3													4	3	3	3	3
[s.back]	servicio de copias de respaldo (backup)																	4	4	5	4	4
[print]	Servicio de impresión	3		4														3	4	4	3	3
[sst]	Servicio de Soporte Técnico Interno																	4	4	4	4	4
[dns]	Servidor de nombres de dominio																	5	4	5	5	5
[voip]	Telefonia IP																	4	3	3	3	3

INTEGRIDAD

Código	Activo	GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
D	Datos/Información																					
[bd.1]	Base de Datos Atenciones																	4	5	5	5	5
[bd.2]	Base de Datos General																	4	4	4	5	4
[bd.3]	Base de Datos Myzro																	4	5	4	4	4
[bd.4]	Base de Datos Kardex																	5	4	5	5	5
[exe]	Codigo ejecutable																	4	4	4	5	4
[source.1]	Codigo Fuente Atenciones																	4	4	3	4	4
[source.2]	Codigo Fuente Myzro																	5	4	4	4	4
[source.3]	Codigo Fuente Ventas																	5	4	4	4	4
[backup]	Copias de respaldo																	5	4	4	4	4
[password]	Crdenciales (contraseñas)																	4	4	4	4	4
[conf]	Datos de configuración																	4	3	3	3	3
[acl]	Datos de control de acceso																	5	4	5	5	5
[test]	Datos de prueba																	4	3	3	3	3
[files]	Ficheros																	4	4	4	4	4
[hc]	Historias Clinicas												5					4	5	5	5	5
S	Servicios																					
[file]	Almacenamiento de ficheros																	5	5	4	5	5
[email]	Correo electrónico Institucion	5	5	5	5	4	4	4	5	4	4	4	4	4	4	5	4	4	5	5	5	4
[www]	Internet	5	5	5	5	4	5	5	5	5	4	5	5	5	5	4	3	4	4	5	5	5
[cont]	Proveedores de T.I	5		5	3													3	3	3	3	3
[s.back]	servicio de copias de respaldo (backup)																	4	4	5	4	4
[print]	Servicio de impresión	3		4														3	4	4	3	3
[sst]	Servicio de Soporte Técnico Interno																	5	4	5	4	5
[dns]	Servidor de nombres de dominio																	3	3	3	5	3
[voip]	Telefonia IP																	4	3	3	3	3

DISPONIBILIDAD

Código	Activo	GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
D	Datos/Información																					
[bd.1]	Base de Datos Atenciones																	5	5	5	5	5
[bd.2]	Base de Datos General																	5	5	5	5	5
[bd.3]	Base de Datos Myzro																	5	5	5	5	5
[bd.4]	Base de Datos Kardex																	5	4	5	5	5
[exe]	Codigo ejecutable																	5	4	4	4	4
[source.1]	Codigo Fuente Atenciones																	5	5	3	4	5
[source.2]	Codigo Fuente Myzro																	4	5	5	5	5
[source.3]	Codigo Fuente Ventas																	4	4	4	5	4
[backup]	Copias de respaldo																	5	5	4	5	5
[password]	Crdenciales (contraseñas)																	4	4	4	4	4
[conf]	Datos de configuración																	3	4	3	4	3
[acl]	Datos de control de acceso																	5	4	5	5	5
[test]	Datos de prueba																	3	4	3	3	3
[files]	Ficheros																	4	3	4	4	4
[hc]	Historias Clinicas													5				4	4	4	5	4
S	Servicios																					
[file]	Almacenamiento de ficheros																	5	5	4	5	5
[email]	Correo electrónico Institucion	4	5	4	4	4	4	4	4	4	5	5	5	4	5	5	5	5	5	5	5	5
[www]	Internet	5	5	5	4	4	5	5	5	5	4	5	5	4	5	4	3	4	4	5	5	5
[cont]	Proveedores de T.I	5		5	3													4	4	3	4	4
[s.back]	servicio de copias de respaldo (backup)																	4	4	5	4	4
[print]	Servicio de impresión	3		4														3	4	4	3	3
[sst]	Servicio de Soporte Técnico Interno																	5	4	5	5	5
[dns]	Servidor de nombres de dominio																	5	4	4	4	4
[voip]	Telefonia IP																	4	4	4	3	4

VALORACION DE ACTIVOS POR PERSONAL INVOLUCRADO CON EL ACTIVO

CONFIDENCIALIDAD

		GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
SW	Aplicaciones/Software																					
[browser.1]	Google Chrome	5	3	5	4	4	4	5	5	5	4	3	3	3	3	3	3	5	5	5	5	5
[browser.2]	Internet Explorer	3	3	3	2	2	3	2	2	3	5	3	2	4	3	2	5	3	2	2	2	2
[av]	Mcafee	5	5	5	4	4	4	4	4	3	3	3	4	5	5	5	4	5	5	5	5	5
[office]	Microsof Office	3	3	3	4	4	3	3	4	5	2	2	5	2	5	5	3	2	2	2	2	2
[dbms.1]	MySQL																	5	5	5	5	5
[dbms.2]	Oracle																	5	5	5	5	5
[prp.1]	Sistema Atenciones	5									5							4	3	4	3	5
[a.back]	Sistema de backup																	4	5	5	5	5
[prp.2]	Sistema Myzro																	5	5	5	4	5
[prp.3]	Sistema Kardex																	4	4	4	4	4
[prp.4]	Sistemas General																	5	4	4	4	4
[dbms.3]	SQL Server 2008																	4	4	4	4	4
[dbms.4]	Visual Fox Pro																	3	4	3	3	3
[windows.1]	Windows 7	5	5	5	4	4	3	4	2	2	5	2	3	4	5	2	4	5	5	5	4	5
[windows.2]	Windows XP														4			2	2	3	2	2
HW	Equipos Informáticos																					
[print	Impresora	3	3	4	5	4	4	4	5	3	3	4	5	2	3	5	5	3	3	3	3	3
[pc.1]	PC Administrativos General	3	4	4	4	3	5	5	5	5	3	3	4	3	2	5	5	4	3	4	3	3
[pc.2]	PC Clinica																	4	4	4	3	4
[pc.3]	PC Gerencia Administrativa	5	5															5	5	4	5	5
[pc.4]	PC Informática																	5	5	5	5	5
[pc.5]	PC Jefaturas			5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	4	5
[scan]	Scanner	1	2	1	3	4	1	3	2	1	2	1	3	2	2	1	2	2	1	1	2	1
[pabx]	Servidor Central Telefónica																	4	4	4	4	4
[servi.1]	Servidor de Backups																	5	4	4	4	4
[servi.2]	Servidor Myzro																	5	5	4	5	5
[switch]	Switches																	3	2	4	2	2

INTEGRIDAD

		GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
SW	Aplicaciones/Software																					
[browser.1]	Google Chrome	5	3	5	4	4	4	5	5	5	4	3	4	4	3	4	3	4	4	4	5	4
[browser.2]	Internet Explorer	4	3	4	2	2	3	5	5	5	4	3	4	4	3	4	4	3	3	3	2	4
[av]	Mcafee	5	5	5	4	4	4	4	4	3	3	3	4	5	5	5	4	5	5	5	5	5
[office]	Microsof Office	3	3	3	4	4	3	3	4	5	2	2	5	2	5	5	3	2	2	2	2	2
[dbms.1]	MySQL																	3	3	4	5	3
[dbms.2]	Oracle																	4	4	4	5	4
[prp.1]	Sistema Atenciones	5									5							4	3	4	3	5
[a.back]	Sistema de backup																	4	5	5	5	5
[prp.2]	Sistema Myzro																	5	5	5	4	5
[prp.3]	Sistema Kardex																	4	4	4	4	4
[prp.4]	Sistemas General																	5	4	4	4	4
[dbms.3]	SQL Server 2008																	4	4	4	4	4
[dbms.4]	Visual Fox Pro																	4	4	4	4	4
[windows.1]	Windows 7	5	5	5	4	4	3	4	2	2	5	2	3	4	5	2	4	5	4	4	4	4
[windows.2]	Windows XP														4			2	2	3	2	2
HW	Equipos Informáticos																					
[print	Impresora	3	3	4	5	4	4	4	5	3	3	4	5	2	3	5	5	3	3	3	3	3
[pc.1]	PC Administrativos General	3	4	4	4	3	5	5	5	5	5	5	4	3	2	5	5	4	4	4	3	5
[pc.2]	PC Clinica																	4	4	4	3	4
[pc.3]	PC Gerencia Administrativa	5	5															5	5	4	5	5
[pc.4]	PC Informática																	5	5	5	5	5
[pc.5]	PC Jefaturas			5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	4	5
[scan]	Scanner	1	2	1	3	3	3	3	2	1	3	3	3	2	2	1	2	2	1	1	2	2
[pabx]	Servidor Central Telefónica																	4	4	4	4	4
[servi.1]	Servidor de Backups																	5	5	5	4	5
[servi.2]	Servidor Myzro																	5	5	4	5	5
[switch]	Switches																	3	2	4	2	2

DISPONIBILIDAD

		GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
SW	Aplicaciones/Software																					
[browser.1]	Google Chrome	5	3	5	4	4	4	5	5	5	4	3	3	3	3	3	3	5	5	5	5	5
[browser.2]	Internet Explorer	3	3	3	2	2	3	2	2	3	5	3	2	4	3	2	5	3	2	2	2	2
[av]	Mcafee	5	5	5	4	4	4	4	4	3	3	3	4	5	5	5	4	5	5	5	5	5
[office]	Microsof Office	3	3	3	4	4	3	3	4	5	2	2	5	2	5	5	3	2	2	2	2	2
[dbms.1]	MySQL																	4	4	4	5	4
[dbms.2]	Oracle																	5	4	4	4	4
[prp.1]	Sistema Atenciones	5									5							4	3	4	3	5
[a.back]	Sistema de backup																	4	5	5	5	5
[prp.2]	Sistema Myzro																	5	5	5	4	5
[prp.3]	Sistema Kardex																	4	4	4	4	4
[prp.4]	Sistemas General																	5	4	4	4	4
[dbms.3]	SQL Server 2008																	3	4	3	3	3
[dbms.4]	Visual Fox Pro																	3	4	3	3	3
[windows.1]	Windows 7	5	5	5	4	4	3	4	2	2	5	2	3	4	5	2	4	5	5	5	4	5
[windows.2]	Windows XP														4			2	2	3	2	2
HW	Equipos Informáticos																					
[print	Impresora	3	3	4	5	4	4	4	5	3	4	4	5	2	4	5	5	4	3	3	3	4
[pc.1]	PC Administrativos General	3	4	4	4	3	5	5	5	4	4	4	4	3	2	5	5	4	3	4	3	4
[pc.2]	PC Clinica																	4	4	4	3	4
[pc.3]	PC Gerencia Administrativa	5	5															4	4	4	4	4
[pc.4]	PC Informática																	5	5	5	5	5
[pc.5]	PC Jefaturas			5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	4	5
[scan]	Scanner	4	2	4	3	4	3	3	4	5	5	1	5	5	5	5	2	3	3	3	3	3
[pabx]	Servidor Central Telefónica																	4	4	4	4	4
[servi.1]	Servidor de Backups																	5	5	5	4	5
[servi.2]	Servidor Myzro																	5	5	4	5	5
[switch]	Switches																	4	4	4	3	4

VALORACION DE ACTIVOS POR PERSONAL INVOLUCRADO CON EL ACTIVO

CONFIDENCIALIDAD

		GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
SI	**Soportes de Información**																					
[san]	Almacenamiento en red	5	4	4	5	4	4	5	4	3	2	5	5	4	2	3	5	5	5	5	5	5
[cca]	Contratos, convenios, y acuer	5	5	5	5	5	4	4	4	5	5	4	5	5	4	5	5	5	5	5	5	5
[printed.1]	Diccionario de Datos																	4	3	5	5	5
[disk.2]	Disco Externo	5																4	5	5	5	5
[printed.2]	Documentacion de los Sistemas																	5	4	4	4	4
[printed.3]	Informes de Auditoria Médica	5														5	5	4	4	5	5	5
[usb]	USB Administrativos General	3	3	4	5	4	4	2	3	1	2	3	1	2	2	3	3	1	1	1	2	3
AUX	**Equipamiento Auxiliar**																					
[ac]	Aires acondicionados	5	4	4	4	2	5	5	3	2	4	4	4	2	3	3	3	5	4	4	5	4
[power]	Fuentes de alimentación																	3	2	3	3	3
[gen]	Generadores eléctricos	5	4	5	2	5	2	4	4	4	5	4	5	4	4	4	3	5	5	5	5	5
[prp.5]	Sistema de control biometrico	4																4	3	3	4	4
[furniture.1]	Stand Madera Oficinas	3	4	5	3	4	5	4	3	5	4	4	5	3	5	4	2	3	3	3	3	3
[furniture.2]	Stand Metálica Oficinas	3	4	5	3	4	5	4	3	5	4	4	5	3	5	4	2	3	3	3	3	3
[ups]	UPS Informática																	4	5	4	4	4
COM	**Redes de Comunicaciones**																					
[WAN]	Red de área amplia																	4	4	4	4	4
[LAN]	Red local																	5	5	4	5	5
[PSTN]	Red telefónica																	3	2	2	2	2
[wifi]	Wifi																	4	3	4	4	4

INTEGRIDAD

		GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
SI	**Soportes de Información**																					
[san]	Almacenamiento en red	5	4	4	5	4	4	5	4	3	2	5	5	4	2	3	5	5	5	5	5	5
[cca]	Contratos, convenios, y acuer	5	5	5	5	5	4	4	4	5	5	4	5	5	4	5	5	4	4	4	4	5
[printed.1]	Diccionario de Datos																	4	3	5	5	5
[disk.2]	Disco Externo	5																4	5	5	5	5
[printed.2]	Documentacion de los Sistemas																	5	4	4	4	4
[printed.3]	Informes de Auditoria Médica	5														5	5	4	4	5	5	5
[usb]	USB Administrativos General	3	3	4	5	4	4	2	3	1	2	3	1	2	2	3	3	1	1	1	2	3
AUX	**Equipamiento Auxiliar**																					
[ac]	Aires acondicionados	5	4	4	4	2	5	5	3	2	4	4	4	2	3	3	3	5	4	4	5	4
[power]	Fuentes de alimentación																	3	2	3	3	3
[gen]	Generadores eléctricos	5	4	5	2	5	2	4	4	4	5	4	5	4	4	4	3	5	5	5	5	5
[prp.5]	Sistema de control biometrico	4																4	3	3	4	4
[furniture.1]	Stand Madera Oficinas	3	4	5	3	4	5	4	3	5	4	4	5	3	5	4	2	3	3	3	3	3
[furniture.2]	Stand Metálica Oficinas	3	4	5	3	4	5	4	3	5	4	4	5	3	5	4	2	3	3	3	3	3
[ups]	UPS Informática																	4	5	4	4	4
COM	**Redes de Comunicaciones**																					
[WAN]	Red de área amplia																	4	4	4	4	4
[LAN]	Red local																	4	4	4	5	4
[PSTN]	Red telefónica																	3	2	2	2	2
[wifi]	Wifi																	4	3	4	4	4

DISPONIBILIDAD

		GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
SI	**Soportes de Información**																					
[san]	Almacenamiento en red	5	4	4	5	4	4	5	4	3	2	5	5	4	2	3	5	5	5	5	5	5
[cca]	Contratos, convenios, y acuer	5	5	5	5	5	4	4	4	5	5	4	5	5	4	5	5	5	5	5	5	5
[printed.1]	Diccionario de Datos																	4	3	5	5	5
[disk.2]	Disco Externo	5																4	5	5	5	5
[printed.2]	Documentacion de los Sistemas																	5	4	4	4	4
[printed.3]	Informes de Auditoria Médica	5														5	5	4	4	5	5	5
[usb]	USB Administrativos General	3	3	4	5	4	4	2	3	1	2	3	1	2	2	3	3	1	1	1	2	3
AUX	**Equipamiento Auxiliar**																					
[ac]	Aires acondicionados	5	4	4	4	2	5	5	3	2	4	4	4	2	3	3	3	5	4	4	5	4
[power]	Fuentes de alimentación																	3	2	3	3	3
[gen]	Generadores eléctricos	5	4	5	2	5	2	4	4	4	5	4	5	4	4	4	3	5	5	5	5	5
[prp.5]	Sistema de control biometrico	4																4	3	3	4	4
[furniture.1]	Stand Madera Oficinas	3	4	5	3	4	5	4	3	5	4	4	5	3	5	4	2	3	3	3	3	3
[furniture.2]	Stand Metálica Oficinas	3	4	5	3	4	5	4	3	5	4	4	5	3	5	4	2	3	3	3	3	3
[ups]	UPS Informática																	4	5	4	4	4
COM	**Redes de Comunicaciones**																					
[WAN]	Red de área amplia																	3	3	4	4	3
[LAN]	Red local																	4	3	3	3	3
[PSTN]	Red telefónica																	3	2	2	2	2
[wifi]	Wifi																	3	2	2	2	2

VALORACION DE ACTIVOS POR PERSONAL INVOLUCRADO CON EL ACTIVO

CONFIDENCIALIDAD

		GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
L	Instalaciones																					
[building.1]	Edificio Clinica																	4	4	5	4	4
[building.2]	Edificio Torre Nueva																	4	4	5	4	4
[local.1]	Oficinas 1 piso													5	5			5	4	5	5	5
[local.2]	Oficinas 2 piso	5	4	5	4			5	4	4								4	4	4	5	4
[local.3]	Oficinas 3 piso					4	4				4	3				3		4	4	4	4	4
[local.4]	Sector Consultorios Medicos Clinica															4	5	4	3	3	3	3
[local.5]	Sector Consultorios Medicos Torre Nueva															4	5	3	4	3	3	3
[local.6]	Sector Historias Clinicas												5			5		4	3	4	4	4
[local.7]	Sector Informatica																	5	5	5	5	5
P	Personal																					
[ui.1]	Administrativos General				4										4							4
[ui.2]	Gerencia Administrativa	5	5																			5
[ui.3]	Jefaturas			5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
[adm]	Administradores de sistemas																	5	5	5	5	5
[des]	Desarrolladores/programadores																	5	5	5	5	5
[ui.4]	Personal Asistencial, Ténicos y Laboratoristas														3							3
[ui.5]	Personal de Auditoria Medica															4						4
[ui.6]	Personal Hist Clinicas												3									3

INTEGRIDAD

		GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
L	Instalaciones																					
[building.1]	Edificio Clinica																	3	3	5	4	3
[building.2]	Edificio Torre Nueva																	3	3	4	4	3
[local.1]	Oficinas 1 piso													3	3			3	3	4	4	3
[local.2]	Oficinas 2 piso	5	4	5	4			5	4	4								4	4	4	5	4
[local.3]	Oficinas 3 piso					4	4				4	3				3		3	3	3	4	3
[local.4]	Sector Consultorios Medicos Clinica															4	5	4	3	3	3	3
[local.5]	Sector Consultorios Medicos Torre Nueva															4	5	3	4	3	3	3
[local.6]	Sector Historias Clinicas												5			5		4	3	4	4	4
[local.7]	Sector Informatica																	5	5	5	5	5
P	Personal																					
[ui.1]	Administrativos General				5										5							5
[ui.2]	Gerencia Administrativa	5	5																			5
[ui.3]	Jefaturas			5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
[adm]	Administradores de sistemas																	5	5	5	5	5
[des]	Desarrolladores/programadores																	5	5	5	5	5
[ui.4]	Personal Asistencial, Ténicos y Laboratoristas														3							3
[ui.5]	Personal de Auditoria Medica															4						4
[ui.6]	Personal Hist Clinicas												3									3

DISPONIBILIDAD

		GA Gerente Adm	SJ Secretaria Jef.	JA Jefa de Adm	JR Jefa RRHH	JAT Jefa Asistencial	JSAC Jefa Cobranzas	JC Jefa Contabilidad	JF Jefa Facturación	JFR Jefa Farmacia	JO Jefa Operaciones	JM Jefe Mantenimiento	JHC Jefe HC	JS Jefa de Servicios	JSAC Jefa de SAC	JAUD Jefa de Aud. Med	GM Gerente Med.	AT1 Asistente Técnico	AT2 Asistente Técnico	AT3 Asistente Técnico	JIT Jefe Sistemas	Total
L	Instalaciones																					
[building.1]	Edificio Clinica																	4	4	5	4	4
[building.2]	Edificio Torre Nueva																	2	2	3	4	2
[local.1]	Oficinas 1 piso													4	4			5	4	5	5	4
[local.2]	Oficinas 2 piso	5	4	5	4			5	4	4								4	4	4	5	4
[local.3]	Oficinas 3 piso					4	4				4	3				3		4	4	4	4	4
[local.4]	Sector Consultorios Medicos Clinica															4	5	4	3	3	3	3
[local.5]	Sector Consultorios Medicos Torre Nueva															4	5	4	4	3	3	4
[local.6]	Sector Historias Clinicas												5			5		4	3	4	4	4
[local.7]	Sector Informatica																	5	5	5	5	5
P	Personal																					
[ui.1]	Administrativos General				4										4							4
[ui.2]	Gerencia Administrativa	5	5																			5
[ui.3]	Jefaturas			5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
[adm]	Administradores de sistemas																	5	5	5	5	5
[des]	Desarrolladores/programadores																	5	5	5	5	5
[ui.4]	Personal Asistencial, Ténicos y Laboratoristas														3							3
[ui.5]	Personal de Auditoria Medica															4						4
[ui.6]	Personal Hist Clinicas												3									3

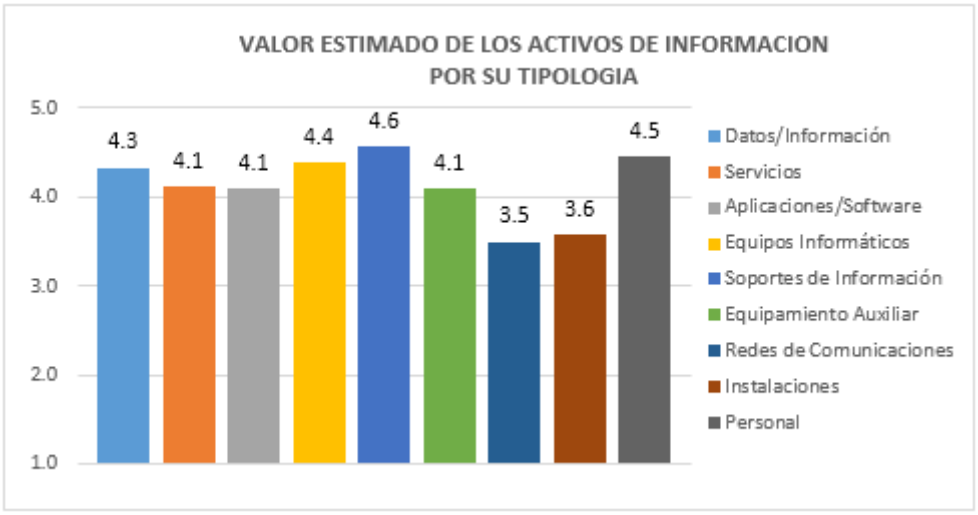
Anexo N° 09: Matriz de Identificación de Amenazas por Comité de análisis

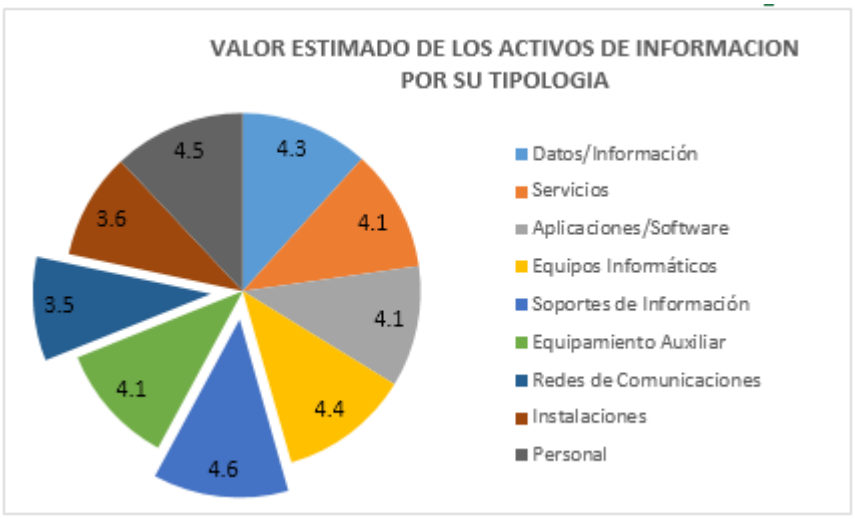
IDENTIFICACION DE AMENAZAS POR PERSONAL INVOLUCRADO		Comité de Analisis de Riesgos																
		GA	SJ	JA	JR	JAT	JSAC	JC	JF	JFR	JO	JM	JHC	JS	JSAC	JAUD	GM	JIT
		Gerente Adm	Secretaria Jef.	Jefa de Adm	Jefa RRHH	Jefa Asistencial	Jefa Cobranzas	Jefa Contabilidad	Jefa Facturación	Jefa Farmacia	Jefa Operaciones	Jefe Mantenimiento	Jefe HC	Jefa de Servicios	Jefa de SAC	Jefa de Aud. Med	Gerente Med.	Jefe Sistemas
N	**Amenazas Naturales**																	
[N.1]	Daños por fuego	x	x	x			x		x		x	x						x
[N.2]	Daños por agua	x	x		x		x	x	x		x	x				x	x	x
[N.3]	Desastres Naturales	x	x									x						
I	**Origen Industrial**																	
[I.1]	Daños por fuego																	
[I.2]	Daños por agua																	
[I.3]	Desastres Industriales																	
[I.4]	Contaminación mecánica	x	x	x	x	x	x	x			x	x					x	x
[I.5]	Contaminación electromagnetica																	
[I.6]	Averías de origen físico o lógico	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x
[I.7]	Corte de suministro eléctrico	x	x			x	x		x		x			x			x	x
[I.8]	Condiciones inadecuadas de temperatura o humedad		x			x			x			x						
[I.9]	Falla de servicios de comunicaciones	x			x	x	x		x								x	x
[I.10]	Interrupción de otros servicios y suministros esenciales		x			x												
[I.11]	Degradación de los soportes de almacenamiento de la información	x	x			x		x										
[I.12]	Emanaciones electromagnéticas																	
E	**Errores y fallos no intencionados**																	
[E.1]	Errores de usuarios	x	x	x	x			x			x		x		x		x	x
[E.2]	Errores de administrador	x	x		x													x
[E.3]	Errores de Monitorización																	x
[E.4]	Errores de Configuración																	x
[E.5]	Deficiencias de la organización			x			x	x	x				x	x			x	x
[E.6]	Disfusión de software dañino	x	x	x	x		x											x
[E.7]	Errores de reencaminamiento																	x
[E.8]	Errores de secuencia																	x
[E.9]	Escapes de información	x	x	x			x		x				x		x			x
[E.10]	Alteración accidental de información							x	x	x	x		x	x	x			x
[E.11]	Destruccion de información				x				x				x				x	
[E.12]	Fugas de información			x		x					x					x	x	
[E.13]	Vulnerabilidad de los programas(software)		x		x													
[E.14]	Errores en mantenimiento / Actualizacion de software	x																x
[E.15]	Errores en mantenimiento / Actualizacion de equipos																	x
[E.16]	Caida de sistema por agotamiento de recursos.		x					x	x			x		x			x	x
[E.17]	Pérdida de equipos	x	x		x								x					
A	**Ataques intencionados**																	
[A.1]	Manipulación de los registros de actividad (log)																	x
[A.2]	Manipulación de la configuración																	x
[A.3]	Suplantación de identidad																	
[A.4]	Abuso de privilegios de acceso																	
[A.5]	Uso no previsto		x			x					x					x		x
[A.6]	Difusión de software dañino	x							x		x					x	x	x
[A.7]	Acceso no autorizado			x	x	x											x	
[A.8]	Repudio																	x
[A.9]	Intercepción de información																	
[A.10]	Modificación deliberada de información																	x
[A.11]	Destrucción de información			x			x				x					x		x
[A.12]	Divulgación de información		x															x
[A.13]	Manipulacion de Programas																	x
[A.14]	Manipulacion de Equipos		x				x				x						x	x
[A.15]	Denegacion de Servicio			x														x
[A.16]	Robo				x													x
[A.17]	Ataque destructivo																	
[A.18]	Ocupación enemiga																	
[A.19]	Indisponibilidad del personal														x			x
[A.20]	Extorsion																	x
[A.21]	Ingenieria social																	x

Anexo N° 10: Matriz de Identificación de Amenazas por tipo activo

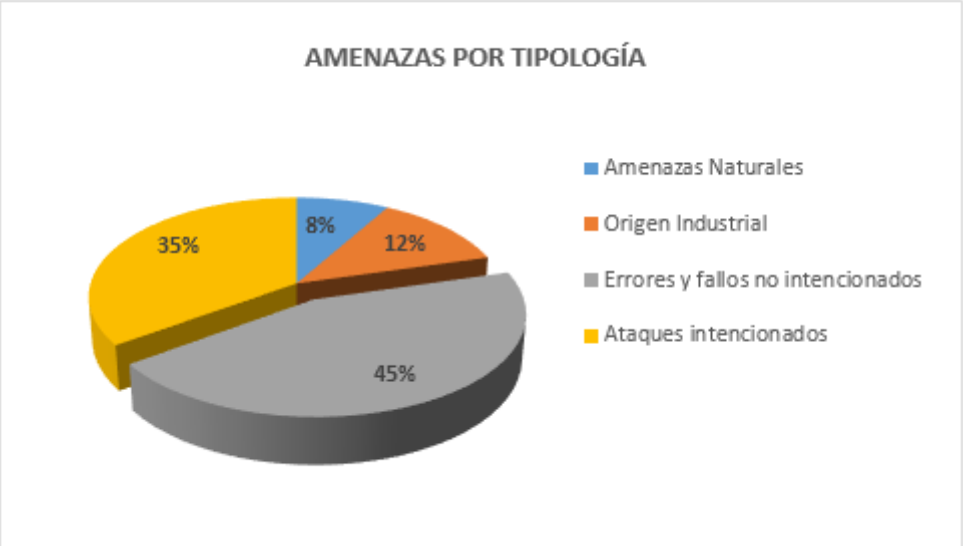
		AMENAZAS	TIPOS DE ACTIVOS									DIMESIONES		
			D	S	SW	HW	SI	AUX	COM	L	P	C	I	D
Amenazas Naturales	[N.1]	Daños por fuego				x	x	x		x				x
	[N.2]	Daños por agua				x	x	x		x				x
	[N.3]	Desastres Naturales				x	x	x		x				x
Origen Industrial	[I.1]	Daños por fuego				x	x	x		x				x
	[I.2]	Daños por agua				x	x	x		x				x
	[I.3]	Desastres Industriales				x	x	x		x				x
	[I.4]	Contaminación mecánica				x	x	x						x
	[I.5]	Contaminación electromagnetica				x	x	x						x
	[I.6]	Averías de origen físico o lógico			x	x	x	x						x
	[I.7]	Corte de suministro eléctrico				x	x	x						x
	[I.8]	Condiciones inadecuadas de temperatura o humedad				x	x	x						x
Errores y fallos no intencionados	[E.1]	Errores de usuarios	x	x	x		x					x	x	x
	[E.2]	Errores de administrador	x	x	x	x	x		x			x	x	x
	[E.3]	Errores de Monitorización	x										x	
	[E.4]	Errores de Configuración	x										x	
	[E.5]	Deficiencias de la organización									x			x
	[E.6]	Disfusión de software dañino			x							x	x	x
	[E.7]	Errores de reencaminamiento		x	x				x			x		
	[E.8]	Errores de secuencia		x	x				x				x	
	[E.9]	Escapes de información										x		
	[E.10]	Alteración accidental de información	x	x	x		x		x	x			x	
	[E.11]	Destruccion de información	x	x	x		x		x	x				x
	[E.12]	Fugas de información	x	x	x		x		x	x	x	x		
	[E.13]	Vulnerabilidad de los programas(software)			x							x	x	x
	[E.14]	Errores en mantenimiento / Actualizacion de software			x								x	x
	[E.15]	Errores en mantenimiento / Actualizacion de equipos				x	x	x						x
	[E.16]	Caida de sistema por agotamiento de recursos.		x		x			x					x
	[E.17]	Pérdida de equipos				x	x	x				x		x
	[E.18]	Indisponibilidad del personal									x			x
Ataques intencionados	[A.1]	Manipulación de los registros de actividad (log)	x										x	
	[A.2]	Manipulación de la configuración	x									x	x	x
	[A.3]	Suplantación de identidad	x	x	x				x			x	x	x
	[A.4]	Abuso de privilegios de acceso	x	x	x	x			x			x	x	x
	[A.5]	Uso no previsto		x	x	x	x	x		x		x	x	x
	[A.6]	Difusión de software dañino			x							x	x	x
	[A.7]	Acceso no autorizado	x	x	x	x	x	x	x	x		x	x	
	[A.8]	Repudio	x	x									x	
	[A.9]	Intercepción de información							x			x		
	[A.10]	Modificación deliberada de información	x	x	x		x		x	x			x	
	[A.11]	Destrucción de información	x	x	x		x			x				x
	[A.12]	Divulgación de información	x	x	x		x		x	x		x		
	[A.13]	Manipulacion de Programas			x							x	x	x
	[A.14]	Manipulacion de Equipos				x	x	x				x		x
	[A.15]	Denegacion de Servicio		x		x			x					x
	[A.16]	Robo				x	x	x				x		x
	[A.17]	Ataque destructivo				x	x	x		x				x
	[A.18]	Ocupación enemiga								x		x		x
	[A.19]	Indisponibilidad del personal									x			x
	[A.20]	Extorsion									x	x	x	x
	[A.21]	Ingenieria social									x	x	x	x

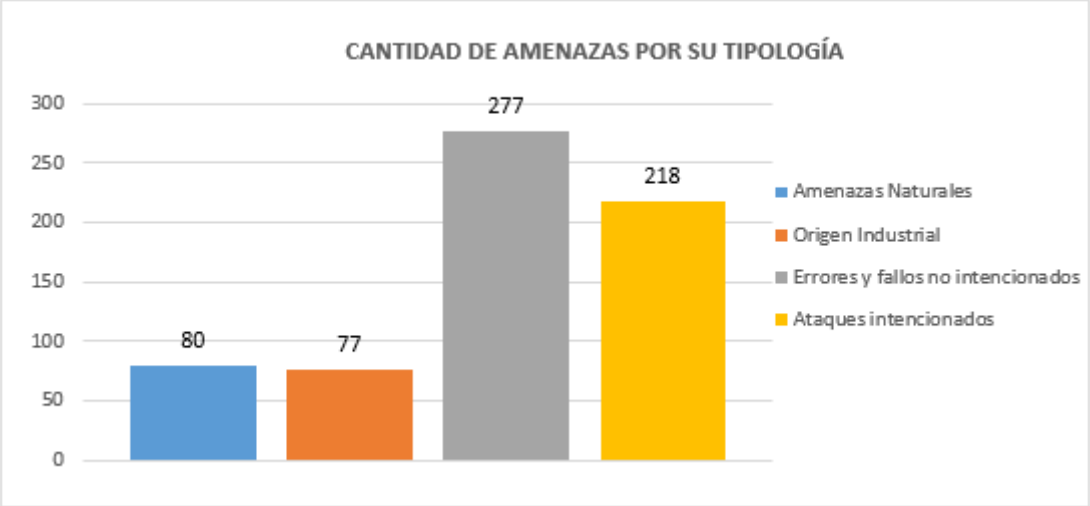
Anexo N° 11: Medición del indicador tipo de activos de la dimensión activos.



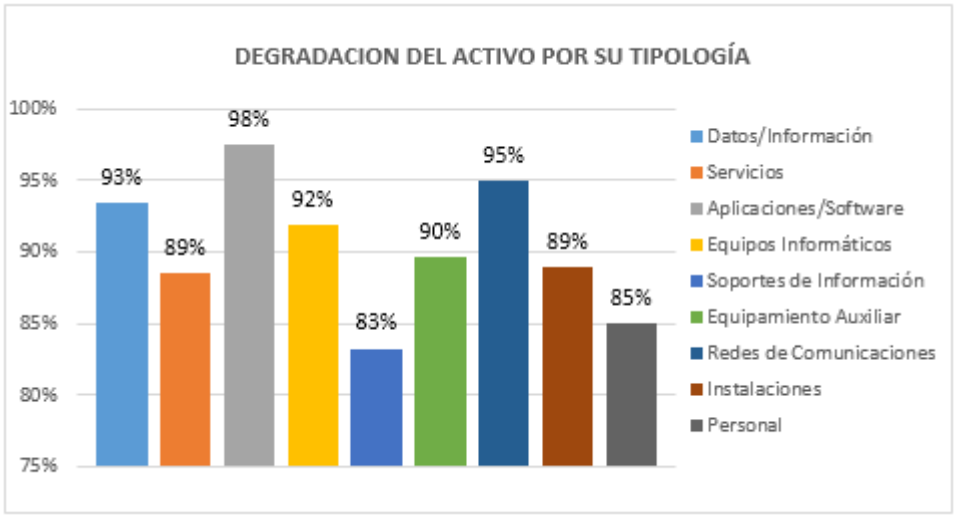


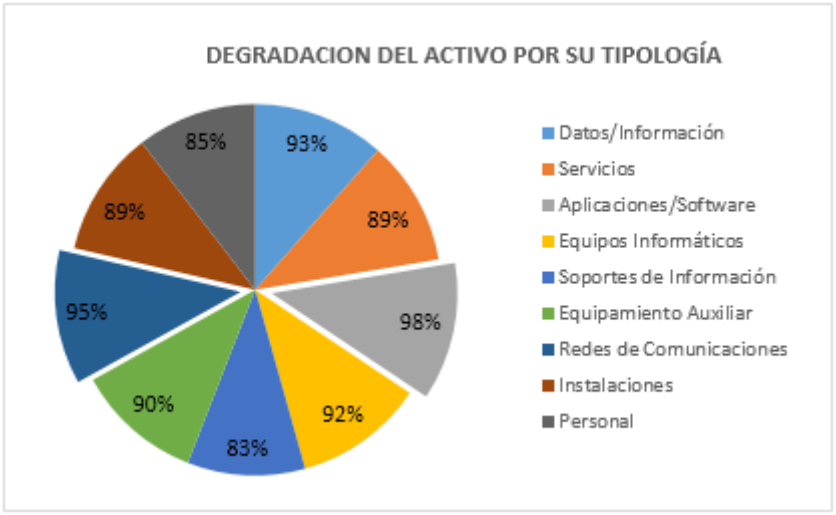
Anexo N° 12: Medición del indicador tipo de amenazas de la dimensión amenazas.



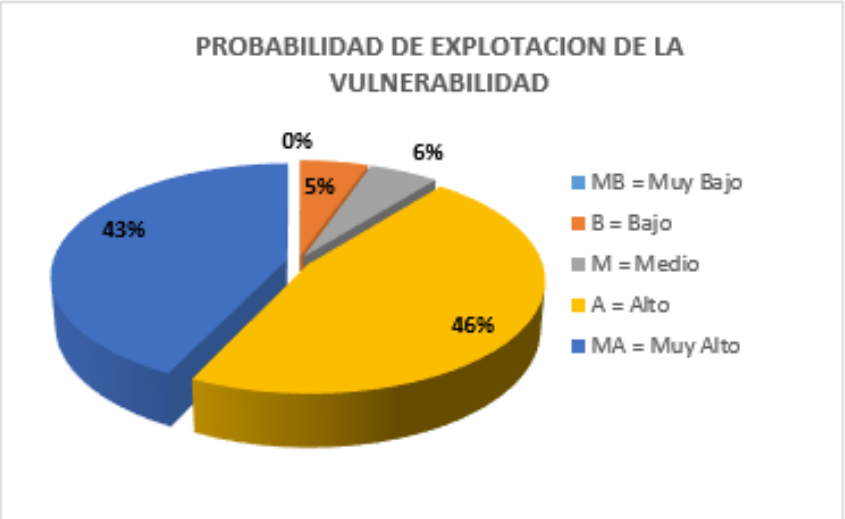


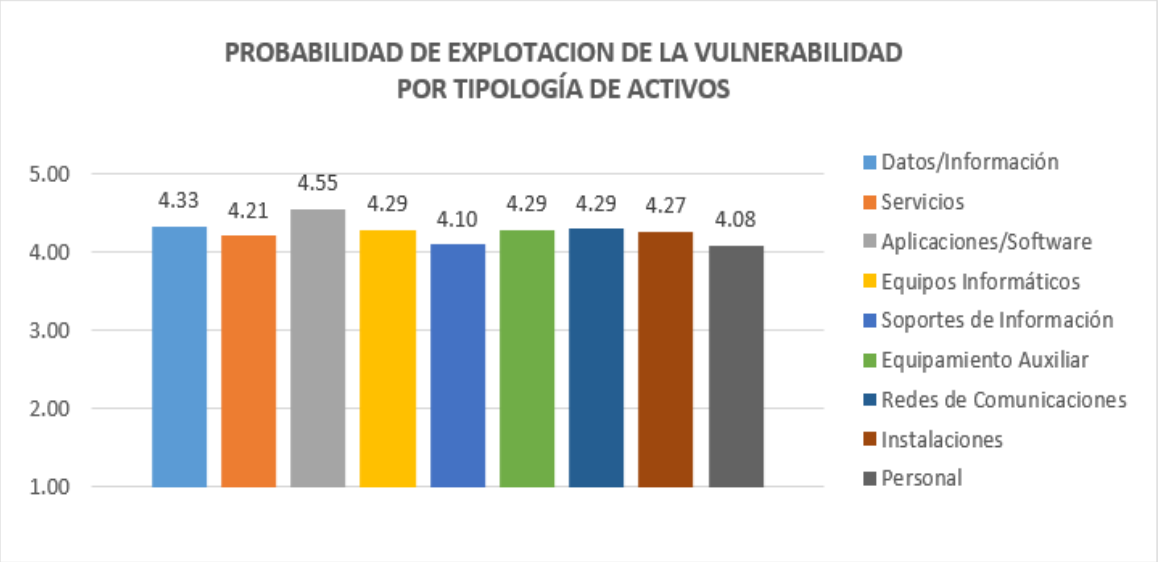
Anexo N° 13: Medición del indicador degradación de la dimensión amenaza.

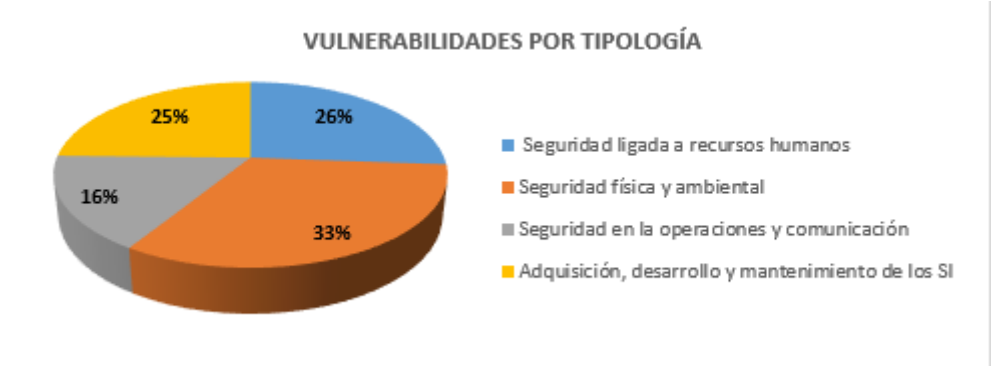




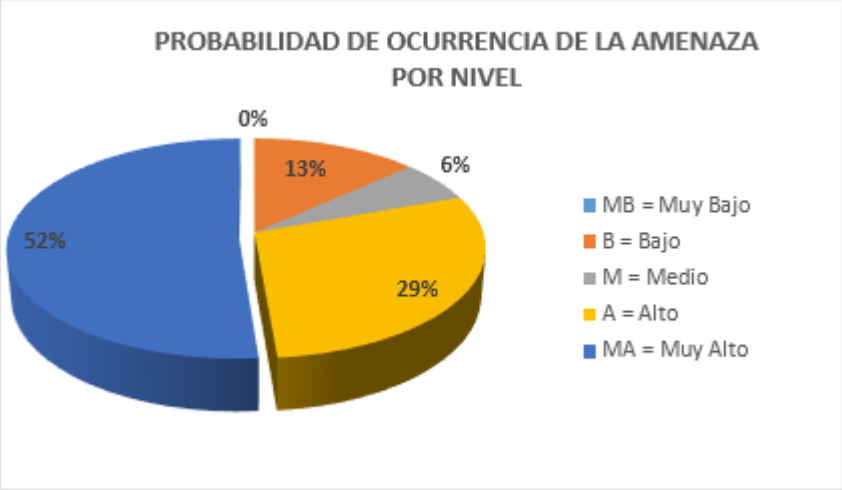
Anexo N° 14: Medición de los indicadores de la dimensión vulnerabilidad.

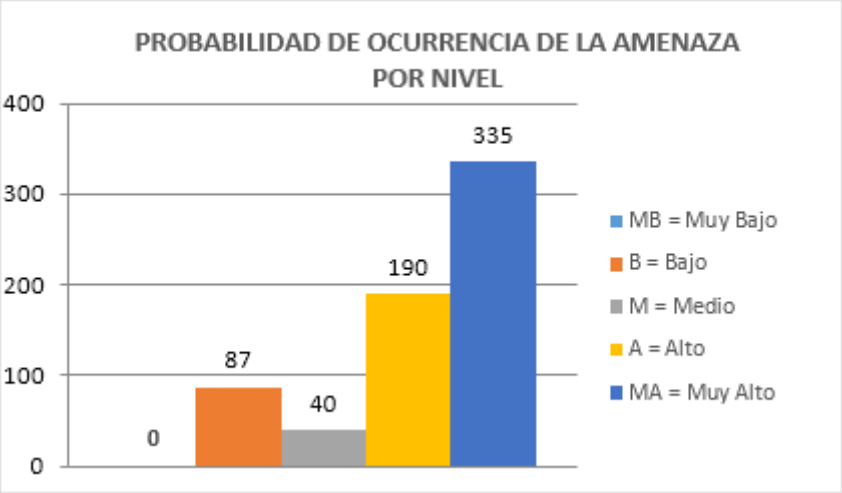




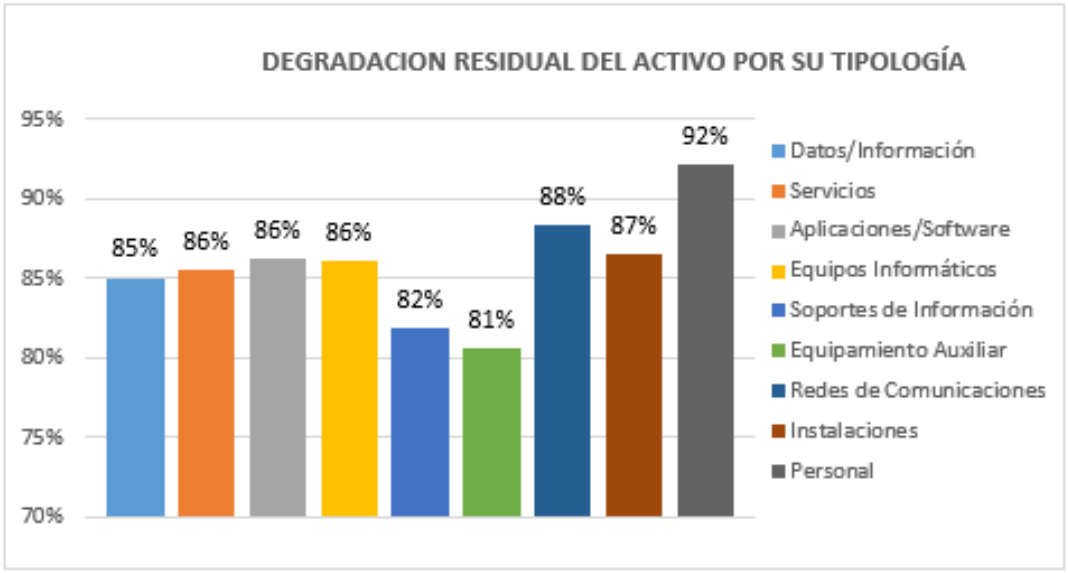


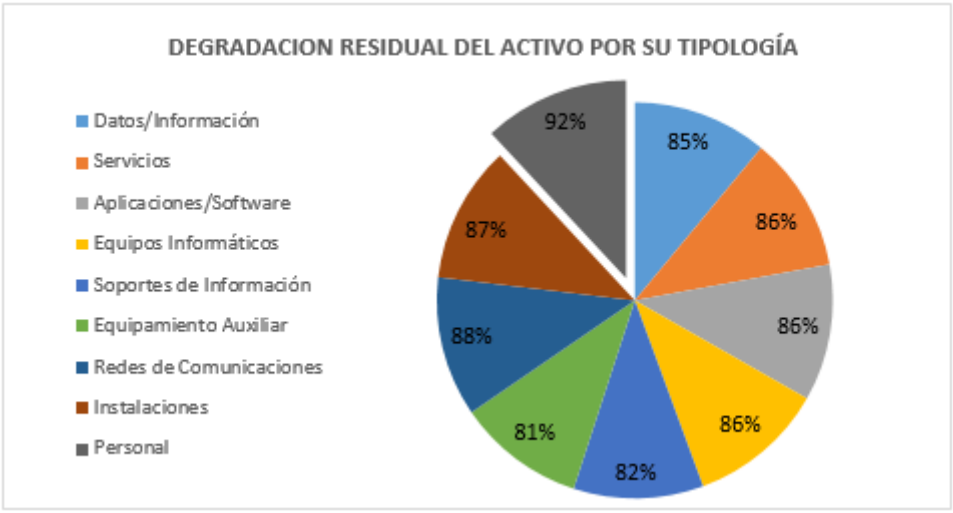
Anexo N° 15: Medición del indicador probabilidad de ocurrencia de la dimensión amenaza.





Anexo N° 16: Medición del indicador degradación residual de la dimensión amenaza.





Anexo N°17 Proyecto De Análisis De Riesgos

CLINICA INTERNACIONAL – PIURA

ANALISIS DE RIESGOS DE LOS ACTIVOS DE INFORMACION APLICANDO LA METODOLOGÍA MAGERIT

Proyecto De Análisis De Riesgos (PAR)

PAR 1.- Actividades Preliminares

PAR 1.1 Estudio de Oportunidad.

Hoy en día la información generada en una organización es muy eminente por ende la seguridad de la misma es requisito fundamental para que una organización funcione correctamente, toda empresa debería estar enmarcada en la seguridad de sus activos de información, pues bien, un análisis de riesgo le permitirá a la misma saber su situación actual en relación a los riesgos a los que se encuentra expuesto sus activos de información, permitiendo salvaguardar sus sistemas de información conjurando dichos riesgos.

PAR 1.2 Determinación del alcance del proyecto

Objetivo General

- Analizar los riesgos de los activos de información identificados en la Clínica Internacional – Piura aplicando la metodología MAGERIT.

Objetivo Específicos

- Identificar y valorar los activos de información de la Clínica Internacional – Piura de acuerdo a la Metodología MAGERIT.
- Determinar y analizar las amenazas identificadas en los activos de información de la Clínica Internacional - Piura aplicando la metodología MAGERIT.
- Determinar y analizar las vulnerabilidades existentes en los activos de información de la Clínica Internacional - Piura aplicando la metodología MAGERIT.
- Proponer las salvaguardas para los activos de información de la Clínica Internacional – Piura aplicando la metodología MAGERIT.

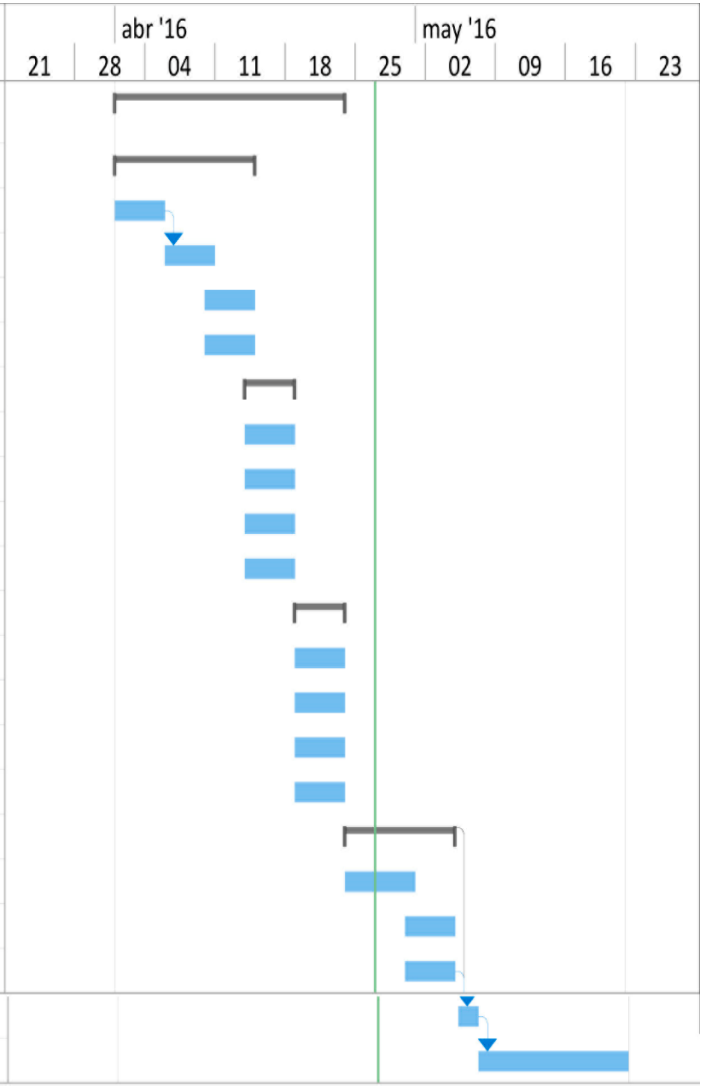
PAR 1.3 Planificación del proyecto

MAGERIT Indica que se debe seleccionar a las personas más importantes dentro de la organización y que conocen de los sistemas de información por tanto el comité estará constituido por dichos colaboradores (Gerencia Administrativa, Jefaturas, Informática, etc.), como se especifican en el cuadro N 01.

Gerencia Administrativa	Gerente Adm	Parte fundamental para la organización, ya que son las personas que tienen la responsabilidad de la organización, y la parte estratégica de la misma
	Secretaria Jef.	
	Jefa de Adm	
Jefaturas	Jefa RRHH	Personal que tienes a su responsabilidad el control y mantenimiento de las área a las que se encuentra asignado teniendo conocimiento de los procesos y de los activos de información que dicho personal tiene a su disposición para la ejecución de sus funciones,
	Jefa Asistencial	
	Jefa Cobranzas	
	Jefa Contabilidad	
	Jefa Facturación	
	Jefa Farmacia	
	Jefa Operaciones	
	Jefe Mantenimiento	
	Jefe HC	
	Jefa de Servicios	
	Jefa de SAC	
	Jefa de Aud. Med	
	Gerente Med.	
Informática	Jefe Sistemas	EL personal del área de TI son aquellas personas que manejan los sistemas y activos de información y tienen gran conocimiento , estratégico, táctico y operativo en la organización
	Asistente Técnico	
	Asistente Técnico	
	Asistente Técnico	

Cuadro N° 01: Comité para el proyecto de análisis de riesgos

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Análisis de Riesgos de los activos de información de la Clínica Internacional – Sede Piura aplicando la metodología**	**23 días**	**vie 01/04/16**	**sáb 23/04/16**
2	**IDENTIFICACION**	**14 días**	**vie 01/04/16**	**jue 14/04/16**
3	**Identificacion de activos**	5 días	vie 01/04/16	mar 05/04/16
4	**Identificacion de amenazas**	5 días	mié 06/04/16	dom 10/04/16
5	**Identificacion de vulnerabilidades**	5 días	dom 10/04/16	jue 14/04/16
6	**Identificacion de Salvaguardas**	5 días	dom 10/04/16	jue 14/04/16
7	**VALORACIONES**	**5 días**	**jue 14/04/16**	**lun 18/04/16**
8	**Valoracion de activos**	5 días	jue 14/04/16	lun 18/04/16
9	**Valoracion de amenazas**	5 días	jue 14/04/16	lun 18/04/16
10	**Valoracion de vulnerabilidades**	5 días	jue 14/04/16	lun 18/04/16
11	**Eficacia de las Salvaguardas**	5 días	jue 14/04/16	lun 18/04/16
12	**ESTIMACIONES**	**5 días**	**mar 19/04/16**	**sáb 23/04/16**
13	**Calculo de Impacto Potencial**	5 días	mar 19/04/16	sáb 23/04/16
14	**Calculo de Riesgo Residual**	5 días	mar 19/04/16	sáb 23/04/16
15	**Calculo de Impacto Residual**	5 días	mar 19/04/16	sáb 23/04/16
16	**Calculo de Riesgo Residual**	5 días	mar 19/04/16	sáb 23/04/16
17	**RESULTADOS**	**11 días**	**dom 24/04/16**	**mié 04/05/16**
18	**Organización de los datos**	7 días	dom 24/04/16	sáb 30/04/16
19	**Análisis de los resultados**	5 días	sáb 30/04/16	mié 04/05/16
20	**Discusión de resultados**	5 días	sáb 30/04/16	mié 04/05/16
21	**CONCLUSIONES Y RECOMENDACIONES**	**2 días**	**jue 05/05/16**	**vie 06/05/16**
22	**ELABORACION DE LA PROPUESTA**	**15 días**	**sáb 07/05/16**	**sáb 21/05/16**



PAR 1.4 Lanzamiento del Proyecto

Para el análisis de riesgos se utilizó una seria de instrumentos que han sido descritos en los anexos anteriores, a la vez se muestran también las diferentes matrices utilizadas para la recopilación de la información.

PAR 2.- Elaboración del análisis de Riesgos

Se define todo el desarrollo del análisis de riesgos de los activos de información por cada una de sus tareas, las mismas que serán observadas a continuación en las siguientes imágenes.

- **Caracterización de los activos de información.**

VALORACION DE ACTIVOS					
Confidencialidad ¿qué daño causaría que el activo lo conociera quien no debe?					C
Integridad ¿qué perjuicio causaría que el activo estuviera dañado o corrupto?					I
Disponibilidad ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?					D
¿De qué manera la perdida del activo afecta la C.I.D.?					
ACTIVOS POR TIPO		Dimensiones			[VE]
		C	I	D	
D	Datos/Información				
[bd.1]	Base de Datos Atenciones	5	5	5	5
[bd.2]	Base de Datos General	4	4	5	4
[bd.3]	Base de Datos Myzro	5	4	5	5
[bd.4]	Base de Datos Kardex	5	5	5	5
[exe]	Codigo ejecutable	5	4	4	4
[source.1]	Codigo Fuente Atenciones	4	4	5	4
[source.2]	Codigo Fuente Myzro	5	4	5	5
[source.3]	Codigo Fuente Ventas	5	4	4	4
[backup]	Copias de respaldo	5	4	5	5
[password]	Credenciales (contraseñas)	3	4	4	4
[conf]	Datos de configuración	4	3	3	3
[acl]	Datos de control de acceso	5	5	5	5
[test]	Datos de prueba	3	3	3	3
[files]	Ficheros	4	4	4	4
[hc]	Historias Clinicas	5	5	4	5
S	Servicios				
[file]	Almacenamiento de ficheros	5	5	5	5
[email]	Correo electrónico Institucional	5	4	5	5
[www]	Internet	5	5	5	5
[cont]	Proveedores de T.I	3	3	4	3
[s.back]	servicio de copias de respaldo (backup)	4	4	4	4
[print]	Servicio de impresión	3	3	3	3
[sst]	Servicio de Soporte Técnico Interno	4	5	5	5
[dns]	Servidor de nombres de dominio	5	3	4	4
[voip]	Telefonía IP	3	3	4	3

SW	Aplicaciones/Software				
[browser.1]	Google Chrome	5	4	5	5
[browser.2]	Internet Explorer	2	4	2	3
[av]	Mcafee	5	5	5	5
[office]	Microsof Office	3	2	3	3
[dbms.1]	MySQL	5	3	4	4
[dbms.2]	Oracle	5	4	4	4
[prp.1]	Sistema Atenciones	5	5	5	5
[a.back]	Sistema de backup	5	5	5	5
[prp.2]	Sistema Myzro	5	5	5	5
[prp.3]	Sistema Kairos	4	4	4	4
[prp.4]	Sistemas General	4	4	4	4
[dbms.3]	SQL Server 2008	4	4	3	4
[windows.1]	Windows 7	5	4	5	5
[windows.2]	Windows XP	3	2	3	3
HW	Equipos Informáticos				
[print.1]	Impresora	3	4	4	4
[pc.1]	PC Administrativos General	5	5	5	5
[pc.2]	PC Clinica	4	5	5	5
[pc.3]	PC Gerencia Administrativa	5	5	4	5
[pc.4]	PC Informática	5	5	5	5
[pc.5]	PC Jefaturas	5	5	5	5
[scan]	Scanner	3	4	4	4
[pabx]	Servidor Central Telefónica	4	4	4	4
[servi.1]	Servidor de Backups	4	5	5	5
[servi.2]	Servidor Myzro	5	5	5	5
[switch]	Switches	2	3	4	3
SI	Soportes de Información				
[san]	Almacenamiento en red	5	5	5	5
[cca]	Contratos, convenios, y acuerdos	5	5	5	5
[printed.1]	Diccionario de Datos	5	5	5	5
[disk.2]	Disco Externo	5	5	5	5
[printed.2]	Documentacion de los Sistemas	4	4	4	4
[printed.3]	Informes de Auditoria Médica	5	5	5	5
[usb]	USB Administrativos General	3	3	3	3
AUX	Equipamiento Auxiliar				
[ac]	Aires acondicionados	4	4	4	4
[power]	Fuentes de alimentación	3	3	5	4
[gen]	Generadores eléctricos	5	5	5	5
[prp.5]	Sistema de control biometrico dactilar y facial	4	5	5	5
[furniture.1]	Stand Madera Oficinas	3	4	4	4
[furniture.2]	Stand Metálica Oficinas	3	4	4	4
[ups]	UPS Informática	4	4	4	4

COM	Redes de Comunicaciones				
[WAN]	Red de área amplia	4	4	3	4
[LAN]	Red local	5	4	3	4
[PSTN]	Red telefónica	2	2	2	3
[wifi]	Wifi	4	4	2	3
L	Instalaciones				
[building.1]	Edificio Clinica	4	3	4	4
[building.2]	Edificio Torre Nueva	4	3	2	3
[local.1]	Oficinas 1 piso	5	3	4	4
[local.2]	Oficinas 2 piso	4	4	4	4
[local.3]	Oficinas 3 piso	4	3	4	4
[local.4]	Sector Consultorios Medicos Clinica	3	3	3	3
[local.5]	Sector Consultorios Medicos Torre Nueva	3	3	4	3
[local.6]	Sector Historias Clinicas	4	4	4	4
[local.7]	Sector Informatica	5	5	5	5
P	Personal				
[ui.1]	Administrativos General	4	5	4	4
[ui.2]	Gerencia Administrativa	5	5	5	5
[ui.3]	Jefaturas	5	5	5	5
[adm]	Administradores de sistemas	5	5	5	5
[des]	Desarrolladores/programadores	5	5	5	5
[ui.4]	Personal Asistencial, Ténicos y Laboratoristas	4	4	3	4
[ui.5]	Personal de Auditoria Medica	4	4	4	4
[ui.6]	Personal Hist Clinicas	3	4	4	4

- **Caracterización de las amenazas**

[backup]	Copias de respaldo	[E.11]	Destruccion de información	5	80%	30%	100%	100%	5
		[E.12]	Fugas de información				30%	80%	4
		[A.11]	Destrucción de información				100%	100%	4
[password]	Credenciales (contraseñas)	[E.11]	Destruccion de información	4	80%	30%	100%	100%	5
		[E.12]	Fugas de información				30%	80%	4
		[A.11]	Destrucción de información				100%	100%	4
[conf]	Datos de configuración	[E.4]	Errores de Configuración	3	80%	30%	80%	80%	5
		[E.11]	Destruccion de información				100%	100%	5
		[E.12]	Fugas de información				30%	80%	5
		[A.11]	Destrucción de información				100%	100%	5
[acl]	Datos de control de acceso	[E.11]	Destruccion de información	5	80%	30%	100%	100%	5
		[E.12]	Fugas de información				30%	80%	4
		[A.11]	Destrucción de información				100%	100%	4
[test]	Datos de prueba	[E.11]	Destruccion de información	3	80%	30%	100%	100%	5
		[E.12]	Fugas de información				30%	80%	4
		[A.11]	Destrucción de información				100%	100%	4
[files]	Ficheros	[E.11]	Destruccion de información	4	80%	30%	100%	100%	5
		[E.12]	Fugas de información				30%	80%	4
		[A.1]	Manipulación de los registros de actividad (log)			100%		100%	3
		[A.11]	Destrucción de información				100%	100%	4
[hc]	Historias Clinicas	[E.11]	Destruccion de información	5	80%	30%	100%	100%	5
		[E.12]	Fugas de información				30%	80%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	3
		[A.11]	Destrucción de información				100%	100%	5
S	**Servicios**								
[file]	Almacenamiento de ficheros	[E.11]	Destruccion de información	5	100%	30%	100%	100%	4
		[E.12]	Fugas de información				30%	100%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	5
		[A.11]	Destrucción de información				80%	80%	4
[email]	Correo electrónico Institucional	[E.1]	Errores de usuarios	5	50%	50%	100%	100%	5
		[E.7]	Errores de reencaminamiento		50%	50%	80%	80%	4
		[E.8]	Errores de secuencia		80%			80%	4
		[E.11]	Destruccion de información				100%	100%	4
		[A.3]	Suplantación de identidad			50%		50%	4
		[A.5]	Uso no previsto		100%	80%	50%	100%	5
		[A.8]	Repudio		30%	30%	50%	50%	3
		[A.15]	Denegacion de Servicio			100%		100%	4
[www]	Internet	[E.2]	Errores de administrador	5	50%	50%	80%	80%	4
		[E.7]	Errores de reencaminamiento		50%	50%	80%	80%	4
		[E.8]	Errores de secuencia		80%			80%	4
		[E.12]	Fugas de información		100%			100%	4
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	4
		[A.5]	Uso no previsto		100%	80%	50%	100%	5
		[A.15]	Denegacion de Servicio				100%	100%	4
[cont]	Proveedores de T.I	[E.11]	Destruccion de información	3			100%	100%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	4
		[A.11]	Destrucción de información				100%	100%	4
		[A.12]	Divulgación de información		100%			100%	5
[s.back]	Servicio de copias de respaldo (b	[E.2]	Errores de administrador	4	50%	50%	80%	80%	4
		[E.12]	Fugas de información		100%			100%	4
		[A.15]	Denegacion de Servicio				100%	100%	4
[print]	Servicio de impresión	[E.1]	Errores de usuarios	3	50%	50%	100%	100%	5
		[A.15]	Denegacion de Servicio				80%	80%	4
[sst]	Servicio de Soporte Técnico Inte	[E.10]	Alteración accidental de información	5		80%		80%	4
[dns]	Servidor de nombres de dominio	[E.10]	Alteración accidental de información	4		80%		80%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	5
		[A.12]	Divulgación de información		100%			100%	4

SW	Aplicaciones/Software								
[browser.1]	Google Chrome	[E.1]	Errores de usuarios	5	50%	50%	80%	80%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.12]	Fugas de información		100%			100%	4
		[A.5]	Uso no previsto		80%	80%	100%	100%	5
[browser.2]	Internet Explorer	[E.1]	Errores de usuarios	3	50%	50%	100%	100%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.12]	Fugas de información		100%			100%	3
		[A.5]	Uso no previsto		80%	80%	100%	100%	5
[av]	Mcafee	[E.1]	Errores de usuarios	5	50%	50%	100%	100%	5
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
[office]	Microsof Office	[E.1]	Errores de usuarios	3	50%	50%	100%	100%	5
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[E.11]	Destruccion de información				100%	100%	4
[dbms.1]	MySQL	[I.6]	Averías de origen físico o lógico	4			100%	100%	5
		[E.1]	Errores de usuarios		50%	50%	100%	100%	5
		[E.2]	Errores de administrador		80%	80%	80%	80%	4
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	5
[office]	Microsof Office	[E.1]	Errores de usuarios	3	50%	50%	100%	100%	5
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[E.11]	Destruccion de información				100%	100%	4
[dbms.1]	MySQL	[I.6]	Averías de origen físico o lógico	4			100%	100%	5
		[E.1]	Errores de usuarios		50%	50%	100%	100%	5
		[E.2]	Errores de administrador		80%	80%	80%	80%	4
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	5
[dbms.2]	Oracle	[I.6]	Averías de origen físico o lógico	4			100%	100%	5
		[E.1]	Errores de usuarios		50%	50%	100%	100%	5
		[E.2]	Errores de administrador		80%	80%	80%	80%	4
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	5
[prp.1]	Sistema Atenciones	[E.1]	Errores de usuarios	5	50%	50%	100%	100%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	4
[a.back]	Sistema de backup	[E.1]	Errores de usuarios	5	50%	50%	100%	100%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	4
[prp.2]	Sistema Myzro	[E.1]	Errores de usuarios	5	50%	50%	100%	100%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	4
[prp.3]	Sistema Ventas	[E.1]	Errores de usuarios	4	50%	50%	100%	100%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	4
[prp.4]	Sistemas General	[E.1]	Errores de usuarios	4	50%	50%	100%	100%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	4
[dbms.3]	SQL Server 2008	[I.6]	Averías de origen físico o lógico	4			100%	100%	5
		[E.1]	Errores de usuarios		50%	50%	100%	100%	5
		[E.2]	Errores de administrador		80%	80%	80%	80%	4
		[E.14]	Errores en mantenimiento / Actualizacion de software			80%	100%	100%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	5
[windows.1]	Windows 7	[E.6]	Disfusión de software dañino	5	80%	80%	100%	100%	5
		[E.1]	Errores de usuarios		50%	50%	100%	100%	5
		[E.11]	Destruccion de información				100%	100%	4
		[E.12]	Fugas de información		100%			100%	3

[windows.2]	Windows XP	[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.1]	Errores de usuarios		50%	50%	100%	100%	5
[pc.4]	PC Informática	[N.1]	Daños por fuego	5			100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[I.4]	Contaminación mecánica				100%	100%	5
		[I.6]	Averías de origen físico o lógico				80%	80%	5
		[I.7]	Corte de suministro eléctrico				50%	50%	5
		[E.1]	Errores de usuarios		50%	50%	100%	100%	5
		[E.4]	Errores de Configuración			80%		80%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.12]	Fugas de información				80%	80%	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	5
		[E.16]	Caida de sistema por agotamiento de recursos.		100%		100%	100%	4
		[E.17]	Pérdida de equipos		100%	100%	100%	100%	5
		[A.2]	Manipulación de la configuración		100%	100%		100%	5
		[A.7]	Acceso no autorizado		100%		50%	100%	4
		[A.14]	Manipulacion de Equipos				80%	80%	5
		[A.16]	Robo		100%		100%	100%	5
[pc.5]	PC Jefaturas	[N.1]	Daños por fuego	5			100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	5
		[I.6]	Averías de origen físico o lógico				80%	80%	5
		[I.7]	Corte de suministro eléctrico				100%	100%	5
		[E.1]	Errores de usuarios		50%	50%	100%	100%	5
		[E.4]	Errores de Configuración			80%		80%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.12]	Fugas de información				80%	80%	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	5
		[E.16]	Caida de sistema por agotamiento de recursos.		100%		100%	100%	4
		[E.17]	Pérdida de equipos		100%	100%	100%	100%	5
		[A.2]	Manipulación de la configuración		100%	100%		100%	4
		[A.7]	Acceso no autorizado		100%		50%	100%	4
		[A.14]	Manipulacion de Equipos				80%	80%	5
		[A.16]	Robo		100%		100%	100%	4
[scan]	Scanner	[I.4]	Contaminación mecánica	4			100%	100%	5
		[I.6]	Averías de origen físico o lógico				100%	100%	5
		[I.7]	Corte de suministro eléctrico				80%	80%	4
		[I.8]	Condiciones inadecuadas de temperatura o humedad				80%	80%	5
		[A.14]	Manipulacion de Equipos		100%		100%	100%	5
		[A.16]	Robo		100%		100%	100%	5
[pabx]	Servidor Central Telefónica	[N.1]	Daños por fuego	4			100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[I.4]	Contaminación mecánica				100%	100%	5
		[I.6]	Averías de origen físico o lógico				80%	80%	5
		[I.7]	Corte de suministro eléctrico				50%	50%	5
		[I.8]	Condiciones inadecuadas				80%	80%	4
		[E.2]	Errores de administrador		80%	80%	100%	100%	5
		[E.4]	Errores de Configuración			80%		80%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.12]	Fugas de información		100%			100%	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				100%	100%	5
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	5
		[E.17]	Pérdida de equipos		100%		100%	100%	4
		[A.4]	Abuso de privilegios de acceso		80%	80%	80%	80%	4
		[A.5]	Uso no previsto		30%	30%	80%	80%	5
		[A.7]	Acceso no autorizado		50%	100%		50%	5
		[A.14]	Manipulacion de Equipos				30%	80%	5
		[A.15]	Denegacion de Servicio				80%	80%	4
		[A.16]	Robo		100%		100%	100%	5
		[A.17]	Ataque destructivo				100%	100%	5

[servi.1]	Servidor de Backups	[N.1]	Daños por fuego	5			100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[I.4]	Contaminación mecánica				100%	100%	5
		[I.6]	Averías de origen físico o lógico				100%	100%	5
		[I.7]	Corte de suministro eléctrico				100%	100%	5
		[I.8]	Condiciones inadecuadas				100%	100%	5
		[E.2]	Errores de administrador		80%	80%	80%	80%	5
		[E.4]	Errores de Configuración			80%		80%	5
		[E.6]	Disfusión de software dañino		80%	80%	100%	100%	5
		[E.12]	Fugas de información		100%			100%	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				100%	100%	5
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	5
		[E.17]	Pérdida de equipos		100%		100%	100%	4
		[A.4]	Abuso de privilegios de acceso		80%	80%	80%	80%	3
		[A.5]	Uso no previsto		30%	30%	80%	80%	4
		[A.7]	Acceso no autorizado		50%	100%		100%	5
		[A.14]	Manipulacion de Equipos				80%	80%	5
		[A.15]	Denegacion de Servicio				80%	80%	5
		[A.16]	Robo		100%		100%	100%	5
		[A.17]	Ataque destructivo				100%	100%	5
[servi.2]	Servidor Myzro	[N.1]	Daños por fuego	5			100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[I.4]	Contaminación mecánica				100%	100%	2
		[I.6]	Averías de origen físico o lógico				100%	100%	5
		[I.7]	Corte de suministro eléctrico				100%	100%	5
		[I.8]	Condiciones inadecuadas				100%	100%	4
		[E.2]	Errores de administrador		30%	30%	80%	80%	5
		[E.4]	Errores de Configuración		50%	50%		50%	5
		[E.6]	Disfusión de software dañino				80%	80%	5
		[E.12]	Fugas de información		100%			100%	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				100%	100%	5
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	5
		[E.17]	Pérdida de equipos		100%		100%	100%	5
		[A.4]	Abuso de privilegios de acceso		80%	80%	80%	80%	4
		[A.5]	Uso no previsto		30%	30%	80%	80%	5
		[A.7]	Acceso no autorizado		50%	100%		100%	5
		[A.14]	Manipulacion de Equipos				80%	80%	5
		[A.15]	Denegacion de Servicio				80%	80%	5
		[A.16]	Robo		100%		100%	100%	5
		[A.17]	Ataque destructivo				100%	100%	5
[switch]	Switches	[N.1]	Daños por fuego	3			100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[I.4]	Contaminación mecánica				100%	100%	5
		[I.6]	Averías de origen físico o lógico				100%	100%	5
		[I.7]	Corte de suministro eléctrico				100%	100%	5
		[I.8]	Condiciones inadecuadas				100%	100%	5
		[E.2]	Errores de administrador		80%	80%	80%	80%	5
		[E.4]	Errores de Configuración		80%	80%	80%	80%	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	5
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	5
		[E.17]	Pérdida de equipos		100%		100%	100%	5
		[A.4]	Abuso de privilegios de acceso		80%	100%	80%	100%	4
		[A.5]	Uso no previsto		30%	100%	50%	100%	5
		[A.7]	Acceso no autorizado		50%	100%		100%	5
		[A.14]	Manipulacion de Equipos				100%	100%	5
		[A.15]	Denegacion de Servicio				80%	80%	5
		[A.16]	Robo		100%		100%	100%	5
		[A.17]	Ataque destructivo				100%	100%	5

SI	Soportes de Información								
[san]	Almacenamiento en red	[E.1]	Errores de usuarios	5	80%	100%	80%	100%	5
		[E.10]	Alteración accidental de información			100%		100%	5
		[A.5]	Uso no previsto		50%	50%	100%	100%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	5
[cca]	Contratos, convenios, y acuerdo	[N.1]	Daños por fuego	5			100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[I.11]	Degradación de los soportes de almacenamiento de la inforr				80%	80%	4
		[E.10]	Alteración accidental de información			50%		50%	2
		[E.11]	Destruccion de información				100%	100%	4
		[E.12]	Fugas de información		80%			80%	4
		[A.7]	Acceso no autorizado		100%	100%		100%	3
		[A.10]	Modificación deliberada de información			100%		100%	3
		[A.11]	Destrucción de información				100%	100%	4
		[A.12]	Divulgación de información		100%			100%	4
		[A.16]	Robo		100%		50%	100%	4
		[A.17]	Ataque destructivo				80%	80%	4
[printed.1]	Diccionario de Datos	[N.1]	Daños por fuego	5			100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[I.4]	Contaminación mecánica				50%	50%	4
		[I.6]	Averías de origen físico o lógico				50%	50%	4
		[I.11]	Degradación de los soportes de almacenamiento de la inforr				80%	80%	4
		[E.10]	Alteración accidental de información			50%		50%	4
		[E.11]	Destruccion de información				100%	100%	4
		[E.12]	Fugas de información		80%			80%	4
		[A.5]	Uso no previsto		80%	80%	50%	80%	4
		[A.7]	Acceso no autorizado		100%	100%		100%	3
		[A.10]	Modificación deliberada de información			50%		50%	3
		[A.11]	Destrucción de información				80%	80%	4
		[A.12]	Divulgación de información		80%			80%	4
		[A.16]	Robo		100%		100%	100%	5
		[A.17]	Ataque destructivo				100%	100%	4
[disk.2]	Disco Externo	[N.1]	Daños por fuego	5			100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[I.4]	Contaminación mecánica				80%	80%	5
		[I.6]	Averías de origen físico o lógico				80%	80%	5
		[I.11]	Degradación de los soportes de almacenamiento de la inforr				80%	80%	4
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información				100%	100%	2
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	5
		[E.17]	Pérdida de equipos		80%		80%	80%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	4
		[A.10]	Modificación deliberada de información			80%		80%	3
		[A.11]	Destrucción de información				80%	80%	3
		[A.14]	Manipulacion de Equipos		80%		80%	80%	4
		[A.16]	Robo		50%		80%	80%	4
		[A.17]	Ataque destructivo				80%	80%	4
[printed.2]	Documentacion de los Sistemas	[N.1]	Daños por fuego	4			100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[I.4]	Contaminación mecánica				50%	50%	4
		[I.6]	Averías de origen físico o lógico				50%	50%	4
		[E.2]	Errores de administrador		80%	80%	80%	80%	4
		[E.10]	Alteración accidental de información			50%		50%	2
		[E.11]	Destruccion de información				100%	100%	2
		[E.12]	Fugas de información		80%			80%	4
		[A.5]	Uso no previsto		80%	80%	50%	80%	4
		[A.7]	Acceso no autorizado		100%	100%		100%	3
		[A.10]	Modificación deliberada de información			50%		50%	3
		[A.11]	Destrucción de información				80%	80%	4

		[A.12]	Divulgación de información		80%			80%	4
		[A.16]	Robo		100%		50%	100%	5
[printed.3]	Informes de Auditoria Médica	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[I.4]	Contaminación mecánica				80%	80%	4
		[I.6]	Averías de origen físico o lógico				80%	80%	4
		[I.11]	Degradación de los soportes de almacenamiento de la inforr				80%	80%	4
		[E.2]	Errores de administrador	5	80%	80%	80%	80%	4
		[E.10]	Alteración accidental de información			50%		50%	2
		[E.11]	Destruccion de información				50%	50%	2
		[A.7]	Acceso no autorizado		100%	100%		100%	3
		[A.10]	Modificación deliberada de información			50%		50%	3
		[A.11]	Destrucción de información				80%	80%	4
		[A.12]	Divulgación de información		80%			80%	4
		[A.16]	Robo		100%		80%	100%	4
[usb]	USB Administrativos General	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[I.4]	Contaminación mecánica				50%	50%	3
		[I.6]	Averías de origen físico o lógico				30%	30%	3
		[E.11]	Destruccion de información	3			30%	30%	2
		[E.12]	Fugas de información		100%			100%	5
		[E.17]	Pérdida de equipos		100%		30%	100%	4
		[A.10]	Modificación deliberada de información			80%		80%	4
		[A.11]	Destrucción de información				80%	80%	4
		[A.16]	Robo		80%		80%	80%	4
AUX	**Equipamiento Auxiliar**								
[ac]	Aires acondicionados	[N.2]	Daños por agua				100%	100%	2
		[I.4]	Contaminación mecánica	4			100%	100%	5
		[I.6]	Averías de origen físico o lógico				100%	100%	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	5
[power]	Fuentes de alimentación	[N.2]	Daños por agua				100%	100%	2
		[I.4]	Contaminación mecánica	4			100%	100%	5
		[I.6]	Averías de origen físico o lógico				100%	100%	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	5
[gen]	Generadores eléctricos	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[I.4]	Contaminación mecánica	5			100%	100%	5
		[I.6]	Averías de origen físico o lógico				100%	100%	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	5
[prp.5]	Sistema de control biometrico d	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[I.4]	Contaminación mecánica				80%	80%	5
		[I.6]	Averías de origen físico o lógico				80%	80%	5
		[I.8]	Condiciones inadecuadas				80%	80%	3
		[I.10]	Interrupción de otros servicios y suministros esenciales	5			100%	100%	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	4
		[E.17]	Pérdida de equipos		50%		50%	50%	4
		[A.7]	Acceso no autorizado		80%	80%		80%	3
		[A.16]	Robo		100%		100%	100%	4
[furniture.1]	Stand Madera Oficinas	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[I.6]	Averías de origen físico o lógico				80%	80%	5
		[I.8]	Condiciones inadecuadas	4			80%	80%	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	4
		[E.17]	Pérdida de equipos		50%		50%	50%	4
		[A.7]	Acceso no autorizado		50%	50%		50%	5
		[A.16]	Robo		100%		100%	100%	4

[furniture.2]	Stand Metálica Oficinas	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[I.6]	Averías de origen físico o lógico				80%	80%	5
		[I.8]	Condiciones inadecuadas	4			80%	80%	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	4
		[E.17]	Pérdida de equipos		50%		50%	50%	4
		[A.7]	Acceso no autorizado		50%	50%		50%	5
		[A.16]	Robo		100%		100%	100%	4
[ups]	UPS Informática	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[I.4]	Contaminación mecánica				100%	100%	5
		[I.6]	Averías de origen físico o lógico				100%	100%	5
		[I.8]	Condiciones inadecuadas				100%	100%	4
		[I.10]	Interrupción de otros servicios y suministros esenciales	4			100%	100%	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos				80%	80%	5
		[E.17]	Pérdida de equipos		100%		100%	100%	4
		[A.7]	Acceso no autorizado		100%	100%		100%	4
		[A.16]	Robo		100%		100%	100%	4
		[A.17]	Ataque destructivo				100%	100%	4
COM	**Redes de Comunicaciones**								
[WAN]	Red de área amplia	[I.9]	Falla de servicios de comunicaciones				100%	100%	4
		[E.2]	Errores de administrador		50%	50%	100%	100%	4
		[E.7]	Errores de reencaminamiento		100%			100%	3
		[E.8]	Errores de secuencia			80%		80%	3
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información				100%	100%	5
		[E.12]	Fugas de información	4	100%			100%	5
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	5
		[A.9]	Intercepción de información		80%			80%	4
		[A.10]	Modificación deliberada de información			100%		100%	4
		[A.12]	Divulgación de información		100%			100%	4
		[A.15]	Denegacion de Servicio				100%	100%	5
[LAN]	Red local	[I.9]	Falla de servicios de comunicaciones				100%	100%	4
		[E.2]	Errores de administrador		50%	50%	100%	100%	4
		[E.7]	Errores de reencaminamiento		100%			100%	3
		[E.8]	Errores de secuencia			80%		80%	3
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información				100%	100%	5
		[E.12]	Fugas de información	4	100%			100%	5
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	5
		[A.9]	Intercepción de información		80%			80%	4
		[A.10]	Modificación deliberada de información			100%		100%	4
		[A.12]	Divulgación de información		100%			100%	4
		[A.15]	Denegacion de Servicio				100%	100%	5
[PSTN]	Red telefónica	[I.9]	Falla de servicios de comunicaciones				100%	100%	4
		[E.2]	Errores de administrador		50%	50%	100%	100%	4
		[E.7]	Errores de reencaminamiento		100%			100%	3
		[E.8]	Errores de secuencia			80%		80%	3
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información				100%	100%	5
		[E.12]	Fugas de información	3	100%			100%	5
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	5
		[A.9]	Intercepción de información		80%			80%	4
		[A.10]	Modificación deliberada de información			100%		100%	4
		[A.12]	Divulgación de información		100%			100%	4
		[A.15]	Denegacion de Servicio				100%	100%	5

[wifi]	Wifi	[I.9]	Falla de servicios de comunicaciones				100%	100%	4
		[E.2]	Errores de administrador		50%	50%	100%	100%	4
		[E.7]	Errores de reencaminamiento		100%			100%	3
		[E.8]	Errores de secuencia			80%		80%	3
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información	3			100%	100%	5
		[E.12]	Fugas de información		100%			100%	5
		[E.16]	Caida de sistema por agotamiento de recursos.				100%	100%	5
		[A.9]	Intercepción de información		80%			80%	4
		[A.10]	Modificación deliberada de información			100%		100%	4
		[A.12]	Divulgación de información		100%			100%	4
		[A.15]	Denegacion de Servicio				100%	100%	5
L	**Instalaciones**								
[building.1]	Edificio Clinica	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información	4			80%	80%	5
		[A.7]	Acceso no autorizado		100%	100%		100%	5
		[A.17]	Ataque destructivo				80%	80%	5
		[A.18]	Ocupación enemiga		80%		100%	100%	3
[building.2]	Edificio Torre Nueva	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información	3			80%	80%	5
		[A.7]	Acceso no autorizado		100%	100%		100%	5
		[A.17]	Ataque destructivo				80%	80%	5
		[A.18]	Ocupación enemiga		80%		100%	100%	3
[local.1]	Oficinas 1 piso	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información				80%	80%	5
		[A.7]	Acceso no autorizado	4	100%	100%		100%	5
		[A.10]	Modificación deliberada de información			80%		80%	5
		[A.11]	Destrucción de información				80%	80%	5
		[A.12]	Divulgación de información		50%			50%	5
		[A.17]	Ataque destructivo				80%	80%	5
		[A.18]	Ocupación enemiga		80%		100%	100%	3
[local.2]	Oficinas 2 piso	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información				80%	80%	5
		[A.7]	Acceso no autorizado	4	100%	100%		100%	5
		[A.10]	Modificación deliberada de información			80%		80%	5
		[A.11]	Destrucción de información				80%	80%	5
		[A.12]	Divulgación de información		50%			50%	5
		[A.17]	Ataque destructivo				80%	80%	5
		[A.18]	Ocupación enemiga		80%		100%	100%	3

[local.3]	Oficinas 3 piso	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información				80%	80%	5
		[A.7]	Acceso no autorizado	4	100%	100%		100%	5
		[A.10]	Modificación deliberada de información			80%		80%	5
		[A.11]	Destrucción de información				80%	80%	5
		[A.12]	Divulgación de información		50%			50%	5
		[A.17]	Ataque destructivo				80%	80%	5
		[A.18]	Ocupación enemiga		80%		100%	100%	3
[local.4]	Sector Consultorios Medicos Clinica	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información				80%	80%	5
		[A.7]	Acceso no autorizado	3	100%	100%		100%	5
		[A.10]	Modificación deliberada de información			80%		80%	5
		[A.11]	Destrucción de información				80%	80%	5
		[A.12]	Divulgación de información		50%			50%	5
		[A.17]	Ataque destructivo				80%	80%	5
		[A.18]	Ocupación enemiga		80%		100%	100%	3
[local.5]	Sector Consultorios Medicos Torre Nueva	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información				80%	80%	5
		[A.7]	Acceso no autorizado	3	100%	100%		100%	5
		[A.10]	Modificación deliberada de información			80%		80%	5
		[A.11]	Destrucción de información				80%	80%	5
		[A.12]	Divulgación de información		50%			50%	5
		[A.17]	Ataque destructivo				80%	80%	5
		[A.18]	Ocupación enemiga		80%		100%	100%	3
[local.6]	Sector Historias Clinicas	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[E.10]	Alteración accidental de información			80%		80%	5
		[E.11]	Destruccion de información				80%	80%	5
		[A.7]	Acceso no autorizado	4	100%	100%		100%	5
		[A.11]	Destrucción de información				80%	80%	5
		[A.12]	Divulgación de información		50%			50%	5
		[A.17]	Ataque destructivo				80%	80%	5
		[A.18]	Ocupación enemiga		80%		100%	100%	3
[local.7]	Sector Informatica	[N.1]	Daños por fuego				100%	100%	2
		[N.2]	Daños por agua				100%	100%	2
		[N.3]	Desastres Naturales				100%	100%	2
		[E.10]	Alteración accidental de información			100%		100%	5
		[E.11]	Destruccion de información				100%	100%	5
		[A.7]	Acceso no autorizado	5	100%	100%		100%	5
		[A.10]	Modificación deliberada de información			100%		100%	5
		[A.11]	Destrucción de información				80%	80%	5
		[A.12]	Divulgación de información		100%			100%	5
		[A.17]	Ataque destructivo				100%	100%	5
		[A.18]	Ocupación enemiga		80%		100%	100%	3

P	Personal								
[ui.1]	Administrativos General	[E.5]	Deficiencias de la organización	4	80%		80%	80%	5
		[E.12]	Fugas de información					80%	4
		[E.18]	Indisponibilidad del personal				80%	80%	4
		[A.19]	Indisponibilidad del personal				100%	100%	5
[ui.2]	Gerencia Administrativa	[E.5]	Deficiencias de la organización	5	80%		80%	80%	5
		[E.12]	Fugas de información					80%	4
		[E.18]	Indisponibilidad del personal				80%	80%	4
		[A.19]	Indisponibilidad del personal				100%	100%	5
[ui.3]	Jefaturas	[E.5]	Deficiencias de la organización	5	80%		80%	80%	5
		[E.12]	Fugas de información					80%	4
		[E.18]	Indisponibilidad del personal				80%	80%	4
		[A.19]	Indisponibilidad del personal				100%	100%	5
[adm]	Administradores de sistemas	[E.5]	Deficiencias de la organización	5	80%		80%	80%	5
		[E.12]	Fugas de información					80%	4
		[E.18]	Indisponibilidad del personal				80%	80%	4
		[A.19]	Indisponibilidad del personal				100%	100%	5
[des]	Desarrolladores/ programadores	[E.5]	Deficiencias de la organización	5	80%		80%	80%	5
		[E.12]	Fugas de información					80%	4
		[E.18]	Indisponibilidad del personal				80%	80%	4
		[A.19]	Indisponibilidad del personal				100%	100%	5
[ui.4]	Personal Asistencial, Ténicos y Laboratoristas	[E.5]	Deficiencias de la organización	4	80%		80%	80%	5
		[E.12]	Fugas de información					80%	4
		[E.18]	Indisponibilidad del personal				80%	80%	4
		[A.19]	Indisponibilidad del personal				100%	100%	5
[ui.5]	Personal de Auditoria Medica	[E.5]	Deficiencias de la organización	4	80%		80%	80%	5
		[E.12]	Fugas de información					80%	4
		[E.18]	Indisponibilidad del personal				80%	80%	4
		[A.19]	Indisponibilidad del personal				100%	100%	5
[ui.6]	Personal Hist Clinicas	[E.5]	Deficiencias de la organización	4	80%		80%	80%	5
		[E.12]	Fugas de información					80%	4
		[E.18]	Indisponibilidad del personal				80%	80%	4
		[A.19]	Indisponibilidad del personal				100%	100%	5

- **Caracterización de vulnerabilidades.**

VALORACION DE VULNERABILIDAD					
Probabilidad de Ocurrencia de una amenza sobre un activo : ¿Cuán probable o improbable es que la amenaza explote la vulnerabilidad?					[PEV]
¿De qué manera la perdida del activo afecta la C.I.D.?					
ACTIVOS POR TIPO		AMENAZAS		VULNERABILIDADES	PEV
D	Datos/Información				
[bd.1]	Base de Datos Atenciones	[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Especificaciones confusas o incompletas para los desarrolladores	5
		[E.4]	Errores de Configuración	Carencia de pruebas de software	4
				Falta de control eficiente del cambio de configuración	4
				Falta de manuales de configuración	5
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Nivel inapropiado de protección criptográfica	4
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
[bd.2]	Base de Datos General	[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Especificaciones confusas o incompletas para los desarrolladores	5
		[E.4]	Errores de Configuración	Carencia de pruebas de software	4
				Falta de control eficiente del cambio de configuración	4
				Falta de manuales de configuración	5
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
		[A.7]	Acceso no autorizado	Carencia de Politicas o reglamento interno	5
				Nivel inapropiado de protección criptográfica	4
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	4
				Falta de políticas de contratación	4

[bd.3]	Base de Datos Myzro	[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	5
				Especificaciones confusas o incompletas para los desarrolladores	5
		[E.4]	Errores de Configuración	Carencia de pruebas de software	4
				Falta de control eficiente del cambio de configuración	4
				Mala Administración de BD	3
				Falta de manuales de configuración	5
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
				Falta de políticas de contratación	4
		[A.7]	Acceso no autorizado	Atribución incorrecta de privilegios de acceso	3
				Carencia de Politicas o reglamento interno	5
				Nivel inapropiado de protección criptográfica	4
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	4
				Falta de políticas de contratación	4
[bd.4]	Base de Datos Ventas	[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Especificaciones confusas o incompletas para los desarrolladores	5
		[E.4]	Errores de Configuración	Carencia de pruebas de software	4
				Falta de control eficiente del cambio de configuración	4
				Falta de manuales de configuración	5
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Atribución incorrecta de privilegios de acceso	3
				Carencia de Politicas o reglamento interno	5
				Nivel inapropiado de protección criptográfica	4
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	4
				Falta de políticas de contratación	4
[exe]	Codigo ejecutable	[E.2]	Errores de administrador	Carencia de pruebas de software	4
				Falta de manuales de configuración	5
		[E.3]	Errores de Monitorización	Falta de mecanismos de monitoreo	3
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
				Falta de planes y procedimientos de continuidad de negocio	5

[source.1]	Codigo Fuente Atenciones	[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Especificaciones confusas o incompletas para los desarrolladores	5
		[E.4]	Errores de Configuración	Carencia de pruebas de software	4
				Falta de control eficiente del cambio de configuración	4
				Falta de manuales de configuración	5
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Atribución incorrecta de privilegios de acceso	3
				Carencia de Politicas o reglamento interno	5
				Nivel inapropiado de protección criptográfica	4
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	4
				Falta de políticas de contratación	4
[source.2]	Codigo Fuente Myzro	[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Especificaciones confusas o incompletas para los desarrolladores	5
		[E.4]	Errores de Configuración	Carencia de pruebas de software	4
				Falta de control eficiente del cambio de configuración	4
				Falta de manuales de configuración	5
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
				Falta de capacitación del personal en uso de aplicaciones	5
				Manejo inadecuado de la red	5
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	5
				Atribución incorrecta de privilegios de acceso	3
				Carencia de Politicas o reglamento interno	5
				Nivel inapropiado de protección criptográfica	4
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
				No planes de contingencia en caso de desastres	5
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	4

[source.3]	Codigo Fuente Ventas	[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Especificaciones confusas o incompletas para los desarrolladores	5
		[E.4]	Errores de Configuración	Carencia de pruebas de software	4
				Falta de control eficiente del cambio de configuración	4
				Falta de manuales de configuración	5
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
				Falta de capacitación del personal en uso de aplicaciones	5
				Manejo inadecuado de la red	5
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
		[A.7]	Acceso no autorizado	Carencia de Politicas o reglamento interno	5
				Nivel inapropiado de protección criptográfica	4
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
				Dejar en sesión el sistema al salir del workstation.	4
				No planes de contingencia en caso de desastres	5
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	4
				Falta de políticas de contratación	4
[backup]	Copias de respaldo	[E.11]	Destruccion de información	No planes de contingencia en caso de desastres	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.11]	Destrucción de información	Acceso no autorizado a los ordenadores	4
				Copiado incontrolado	4
[password]	Credenciales (contraseñas)	[E.11]	Destruccion de información	Falta de copias back-up	5
				Protección de datos y privacidad de la información personal baja	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.11]	Destrucción de información	Acceso no autorizado a los ordenadores	4
				Copiado incontrolado	4
[conf]	Datos de configuración	[E.4]	Errores de Configuración	Carencia de pruebas de software	4
				Falta de control eficiente del cambio de configuración	4
				Falta de manuales de configuración	5
		[E.11]	Destruccion de información	Falta de copias back-up	5
		[E.12]	Fugas de información	Falta de sensibilización	4
		[A.11]	Destrucción de información	Acceso no autorizado a los ordenadores	4
				Copiado incontrolado	4
[acl]	Datos de control de acceso	[E.11]	Destruccion de información	Administración pobre de contraseñas	4

[backup]	Copias de respaldo	[E.11]	Destruccion de información	No planes de contingencia en caso de desastres	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.11]	Destrucción de información	Acceso no autorizado a los ordenadores	4
				Copiado incontrolado	4
[password]	Credenciales (contraseñas)	[E.11]	Destruccion de información	Falta de copias back-up	5
				Protección de datos y privacidad de la información personal baja	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.11]	Destrucción de información	Acceso no autorizado a los ordenadores	4
				Copiado incontrolado	4
[conf]	Datos de configuración	[E.4]	Errores de Configuración	Carencia de pruebas de software	4
				Falta de control eficiente del cambio de configuración	4
				Falta de manuales de configuración	5
		[E.11]	Destruccion de información	Falta de copias back-up	5
		[E.12]	Fugas de información	Falta de sensibilización	4
		[A.11]	Destrucción de información	Acceso no autorizado a los ordenadores	4
				Copiado incontrolado	4
[acl]	Datos de control de acceso	[E.11]	Destruccion de información	Administración pobre de contraseñas	4
		[E.12]	Fugas de información	Falta de sensibilización	4
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
[test]	Datos de prueba	[E.11]	Destruccion de información	Acceso no autorizado a los ordenadores	4
				Copiado incontrolado	4
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.11]	Destrucción de información	Insuficiente mantenimiento / mala instalación de los medios de almacenaje.	4
[files]	Ficheros	[E.11]	Destruccion de información	Acceso no autorizado a las librerías fuente de los programas	2
				Falta de copias back-up	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.1]	Manipulación de los registros de acti	Falta de manuales de configuración	5
		[A.11]	Destrucción de información	Conexiones de red pública desprotegidas	4
[hc]	Historias Clinicas	[E.11]	Destruccion de información	Protección de datos y privacidad de la información personal	4
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	5
				Carencia de Politicas o reglamento interno	5
				Carencia de proteccion externa a las instalaciones	5
				Falta de control de acceso a oficinas o salones restringidos	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
		[A.11]	Destrucción de información	Protección de datos y privacidad de la información personal	4
				Acceso físico no autorizado	5

S	Servicios				
[file]	Almacenamiento de ficheros	[E.11]	Destruccion de información	Acceso no autorizado a las librerías fuente de los programas	2
				Código malicioso	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[A.7]	Acceso no autorizado	Acceso no autorizado a la documentación del sistema	4
		[A.11]	Destrucción de información	Acceso físico no autorizado	4
[email]	Correo electrónico Institucional	[E.1]	Errores de usuarios	Falta de capacitación del personal en uso de aplicaciones	5
				Falta políticas de uso de aplicaciones y de información	4
				Uso Incorrecto del hardware y software	4
		[E.7]	Errores de reencaminamiento	Conexiones de red pública desprotegidas	4
				Falta de identificación y autentificación del remitente y del receptor	4
				Falta de políticas para el uso correcto de los medios de telecomunicación y mensajería	4
				Falta de pruebas de envío y recibimiento del mensaje	4
		[E.8]	Errores de secuencia	Falta de identificación y autentificación del remitente y del receptor	4
		[E.11]	Destruccion de información	Dejar en sesión el sistema al salir del workstation.	4
				Protección de datos y privacidad de la información personal	4
		[A.3]	Suplantación de identidad	Administración pobre de contraseñas	4
				Atribución incorrecta de privilegios de acceso	3
		[A.5]	Uso no previsto	Descarga y uso incontrolado de software	4
		[A.8]	Repudio	Carencia de mecanismos de control para el envio/recepeción de mensajes	4
		[A.15]	Denegacion de Servicio	Apagones por manipulacion de proveedor	4
[www]	Internet	[E.2]	Errores de administrador	Falta políticas de uso de aplicaciones y de información	4
		[E.7]	Errores de reencaminamiento	Falta de identificación y autentificación del remitente y del receptor	4
				Falta de pruebas de envío y recibimiento del mensaje	4
		[E.8]	Errores de secuencia	Falta de pruebas de envío y recibimiento del mensaje	4
		[E.12]	Fugas de información		4
		[E.16]	Caida de sistema por agotamiento de	Carencia de Politicas o reglamento interno	5
		[A.5]	Uso no previsto	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5
		[A.15]	Denegacion de Servicio	Fallo del sistema	5
				Mala implementación de red	3

[cont]	Proveedores de T.I	[E.11]	Destruccion de información	Código malicioso	5
		[A.7]	Acceso no autorizado	Falta de recursos de proteccion de TI	5
				Nivel inapropiado de protección criptográfica	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	4
				Falta de políticas de contratación	4
[s.back]	Servicio de copias de respaldo (b	[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Falta de manuales de configuración	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5
[print]	Servicio de impresión	[E.1]	Errores de usuarios	Uso Incorrecto del hardware y software	4
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5
[sst]	Servicio de Soporte Técnico Inte	[E.10]	Alteración accidental de información	Uso Incorrecto del hardware y software	4
[dns]	Servidor de nombres de dominio	[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[A.7]	Acceso no autorizado	Código malicioso	5
		[A.12]	Divulgación de información	Falta de políticas de documentacion	4
[voip]	Telefonía IP	[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Especificaciones confusas o incompletas para los desarrolladores	5
		[E.12]	Fugas de información	Falta políticas de uso de aplicaciones y de información	4
				Falta de capacitacion del personal en seguridad	5
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5

SW	Aplicaciones/Software				
[browser.1]	Google Chrome	[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.6]	Disfusión de software dañino	Falta de control de software ilegal o dañino	5
				Código malicioso	5
		[E.12]	Fugas de información	Falta de sensibilización	4
		[A.5]	Uso no previsto	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5
[browser.2]	Internet Explorer	[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.6]	Disfusión de software dañino	Falta de control de software ilegal o dañino	5
				Código malicioso	5
		[E.12]	Fugas de información	Falta de sensibilización	4
		[A.5]	Uso no previsto	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5
[av]	Mcafee	[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.14]	Errores en mantenimiento / Actualiza	Carencia de pruebas de software	4
[office]	Microsof Office	[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.14]	Errores en mantenimiento / Actualiza	Carencia de pruebas de software	4
		[E.11]	Destruccion de información	Dejar en sesión el sistema al salir del workstation.	4
				Atribución incorrecta de privilegios de acceso	3
[dbms.1]	MySQL	[I.6]	Averías de origen físico o lógico	Falta de mecanismos de supervisión	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Uso Incorrecto del hardware y software	4
		[E.14]	Errores en mantenimiento / Actualiza	Carencia de pruebas de software	4
		[A.7]	Acceso no autorizado	Falta de control de software ilegal o dañino	5

[dbms.2]	Oracle	[I.6]	Averías de origen físico o lógico	Falta de mecanismos de supervisión	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Uso Incorrecto del hardware y software	4
		[E.14]	Errores en mantenimiento / Actualiza	Carencia de pruebas de software	4
		[A.7]	Acceso no autorizado	Falta de control de software ilegal o dañino	5
[prp.1]	Sistema Atenciones	[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.6]	Disfusión de software dañino	Código malicioso	5
				Falta de control de software ilegal o dañino	5
		[E.14]	Errores en mantenimiento / Actualiza	Carencia de pruebas de software	4
		[E.16]	Caida de sistema por agotamiento de	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5
[a.back]	Sistema de backup	[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.6]	Disfusión de software dañino	Código malicioso	5
				Falta de control de software ilegal o dañino	5
		[E.14]	Errores en mantenimiento / Actualiza	Carencia de pruebas de software	4
		[E.16]	Caida de sistema por agotamiento de	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5
[prp.2]	Sistema Myzro	[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.6]	Disfusión de software dañino	Código malicioso	5
				Falta de control de software ilegal o dañino	5
		[E.14]	Errores en mantenimiento / Actualiza	Carencia de pruebas de software	4
		[E.16]	Caida de sistema por agotamiento de	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5

[prp.3]	Sistema Ventas	[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.6]	Disfusión de software dañino	Código malicioso	5
				Falta de control de software ilegal o dañino	5
		[E.14]	Errores en mantenimiento / Actualiza	Carencia de pruebas de software	4
		[E.16]	Caida de sistema por agotamiento de	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5
[prp.4]	Sistemas General	[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.6]	Disfusión de software dañino	Código malicioso	5
				Falta de control de software ilegal o dañino	5
		[E.14]	Errores en mantenimiento / Actualiza	Carencia de pruebas de software	4
		[E.16]	Caida de sistema por agotamiento de	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5
[dbms.3]	SQL Server 2008	[I.6]	Averías de origen físico o lógico	Falta de mecanismos de supervisión	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.2]	Errores de administrador	Documentación de software incompleta o mal elaborada	4
				Uso Incorrecto del hardware y software	4
		[E.14]	Errores en mantenimiento / Actualiza	Carencia de pruebas de software	4
		[A.7]	Acceso no autorizado	Falta de control de software ilegal o dañino	5
[windows.1]	Windows 7	[E.6]	Disfusión de software dañino	Código malicioso	5
				Falta de control de software ilegal o dañino	5
		[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.11]	Destruccion de información	Dejar en sesión el sistema al salir del workstation.	4
				Falta de copias back-up	5
		[E.12]	Fugas de información	Falta políticas de uso de aplicaciones y de información	4

[windows.2]	Windows XP	[E.6]	Disfusión de software dañino	Código malicioso	5
				Falta de control de software ilegal o dañino	5
		[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.11]	Destruccion de información	Dejar en sesión el sistema al salir del workstation.	4
				Falta de copias back-up	5
		[E.12]	Fugas de información	Falta políticas de uso de aplicaciones y de información	4
HW	**Equipos Informáticos**				
[print]	Impresora	[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
				Falta de plan de sustitución de equipos	4
		[I.7]	Corte de suministro eléctrico	Apagones por manipulacion de proveedor	4
				Fallo del sistema	5
		[I.8]	Condiciones inadecuadas de tempera	Susceptibilidad a las variaciones de la temperatura	2
				Ubicación de activos en espacios de riesgo	4
		[A.14]	Manipulacion de Equipos	Acceso no autorizado a las infraestructuras informáticas	4
				Administración pobre de contraseñas	4
		[A.16]	Robo	Falta de acondicionamiento para la protección de equipos	4
				Acceso físico no autorizado	4
[pc.1]	PC Administrativos General	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Carencia de un plan de sustitucion de equipos	5
		[I.7]	Corte de suministro eléctrico	Susceptibilidad a las variaciones del voltaje	5
				Apagones por manipulacion de proveedor	4
		[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.4]	Errores de Configuración	Falta de manuales de configuración	5
		[E.6]	Disfusión de software dañino	Falta de control de software ilegal o dañino	5
		[E.12]	Fugas de información	Dejar en sesión el sistema al salir del workstation.	4

		[A.2]	Manipulación de la configuración	Falta de control eficiente del cambio de configuración	4
				Falta de control de acceso a oficinas o salones restringidos	4
		[A.7]	Acceso no autorizado	Falta de control de software ilegal o dañino	5
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
				Administración pobre de contraseñas	4
		[A.16]	Robo	Acceso físico no autorizado	4
				Falta de protección física del edificio, puertas y ventanas	4
[pc.2]	PC Clinica	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Carencia de un plan de sustitucion de equipos	5
		[I.7]	Corte de suministro eléctrico	Susceptibilidad a las variaciones del voltaje	5
				Apagones por manipulacion de proveedor	4
		[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.4]	Errores de Configuración	Falta de manuales de configuración	5
		[E.6]	Disfusión de software dañino	Falta de control de software ilegal o dañino	5
		[E.12]	Fugas de información	Dejar en sesión el sistema al salir del workstation.	4
		[E.15]	Errores en mantenimiento / Actualiza	Fallo del sistema	5
		[E.16]	Caida de sistema por agotamiento de	Manejo inadecuado de la red	5
		[E.17]	Pérdida de equipos	Ausencia de personal	4
				Almacenamiento de producto inflamables	3
				Carencia de control en la entrega de activos al caducar contrato	5
				Incorrecta clasificación, etiquetado o manejo de la información.	4
				Acceso no autorizado a las infraestructuras informáticas	4
		[A.2]	Manipulación de la configuración	Falta de control eficiente del cambio de configuración	4
				Falta de control de acceso a oficinas o salones restringidos	4
		[A.7]	Acceso no autorizado	Falta de control de software ilegal o dañino	5
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
				Administración pobre de contraseñas	4
		[A.16]	Robo	Acceso físico no autorizado	4
				Falta de protección física del edificio, puertas y ventanas	4

[pc.3]	PC Gerencia Administrativa	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Carencia de un plan de sustitucion de equipos	5
		[I.7]	Corte de suministro eléctrico	Susceptibilidad a las variaciones del voltaje	5
				Apagones por manipulacion de proveedor	4
		[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.4]	Errores de Configuración	Falta de manuales de configuración	5
		[E.6]	Disfusión de software dañino	Falta de control de software ilegal o dañino	5
		[E.12]	Fugas de información	Dejar en sesión el sistema al salir del workstation.	4
		[E.15]	Errores en mantenimiento / Actualiza	Fallo del sistema	5
		[E.16]	Caida de sistema por agotamiento de	Manejo inadecuado de la red	5
		[E.17]	Pérdida de equipos	Ausencia de personal	4
				Almacenamiento de producto inflamables	3
				Carencia de control en la entrega de activos al caducar contrato	5
				Incorrecta clasificación, etiquetado o manejo de la información.	4
				Acceso no autorizado a las infraestructuras informáticas	4
		[A.2]	Manipulación de la configuración	Falta de control eficiente del cambio de configuración	4
				Falta de control de acceso a oficinas o salones restringidos	4
		[A.7]	Acceso no autorizado	Falta de control de software ilegal o dañino	5
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
				Administración pobre de contraseñas	4
		[A.16]	Robo	Acceso físico no autorizado	4
				Falta de protección física del edificio, puertas y ventanas	4

[pc.4]	PC Informática	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Carencia de un plan de sustitucion de equipos	5
		[I.7]	Corte de suministro eléctrico	Susceptibilidad a las variaciones del voltaje	5
				Apagones por manipulacion de proveedor	4
		[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.4]	Errores de Configuración	Falta de manuales de configuración	5
		[E.6]	Disfusión de software dañino	Falta de control de software ilegal o dañino	5
		[E.12]	Fugas de información	Dejar en sesión el sistema al salir del workstation.	4
		[E.15]	Errores en mantenimiento / Actualiza	Fallo del sistema	5
		[E.16]	Caida de sistema por agotamiento de	Manejo inadecuado de la red	5
		[E.17]	Pérdida de equipos	Ausencia de personal	4
				Almacenamiento de producto inflamables	3
				Carencia de control en la entrega de activos al caducar contrato	5
				Incorrecta clasificación, etiquetado o manejo de la información.	4
				Acceso no autorizado a las infraestructuras informáticas	4
		[A.2]	Manipulación de la configuración	Falta de control eficiente del cambio de configuración	4
				Falta de control de acceso a oficinas o salones restringidos	4
		[A.7]	Acceso no autorizado	Falta de control de software ilegal o dañino	5
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
		[A.16]	Robo	Acceso físico no autorizado	5
				Falta de protección física del edificio, puertas y ventanas	4

[pc.5]	PC Jefaturas	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Carencia de un plan de sustitucion de equipos	5
		[I.7]	Corte de suministro eléctrico	Susceptibilidad a las variaciones del voltaje	5
				Apagones por manipulacion de proveedor	4
		[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.4]	Errores de Configuración	Falta de manuales de configuración	5
		[E.6]	Disfusión de software dañino	Falta de control de software ilegal o dañino	5
		[E.12]	Fugas de información	Dejar en sesión el sistema al salir del workstation.	4
		[E.15]	Errores en mantenimiento / Actualiza	Fallo del sistema	5
		[E.16]	Caida de sistema por agotamiento de	Manejo inadecuado de la red	5
		[E.17]	Pérdida de equipos	Ausencia de personal	4
				Almacenamiento de producto inflamables	3
				Carencia de control en la entrega de activos al caducar contrato	5
				Incorrecta clasificación, etiquetado o manejo de la información.	4
				Acceso no autorizado a las infraestructuras informáticas	4
		[A.2]	Manipulación de la configuración	Falta de control eficiente del cambio de configuración	4
				Falta de control de acceso a oficinas o salones restringidos	4
		[A.7]	Acceso no autorizado	Falta de control de software ilegal o dañino	5
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
		[A.16]	Robo	Acceso físico no autorizado	5
				Falta de protección física del edificio, puertas y ventanas	4

[scan]	Scanner	[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
				Carencia de un plan de sustitucion de equipos	5
		[I.7]	Corte de suministro eléctrico	Susceptibilidad a las variaciones del voltaje	5
				Apagones por manipulacion de proveedor	4
		[I.8]	Condiciones inadecuadas de tempera	Fuga de agua	2
				Susceptibilidad a la humedad, al polvo	5
				Localización en un área susceptible a la inundación	2
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
		[A.16]	Robo	Acceso físico no autorizado	4
				Falta de protección física del edificio, puertas y ventanas	4
[pabx]	Servidor Central Telefónica	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Carencia de un plan de sustitucion de equipos	5
		[I.7]	Corte de suministro eléctrico	Susceptibilidad a las variaciones del voltaje	5
				Apagones por manipulacion de proveedor	4
		[I.8]	Condiciones inadecuadas	Ubicación de activos en espacios de riesgo	5
		[E.2]	Errores de administrador	Uso Incorrecto del hardware y software	4
				Falta de copias back-up	5
				Documentación de software incompleta o mal elaborada	4
		[E.4]	Errores de Configuración	Falta de manuales de configuración	5
		[E.6]	Disfusión de software dañino	Código malicioso	5
				Disposición o reutilización de los medios de almacenaje sin una apropiada verificación	3
				Falta de control de software ilegal o dañino	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[E.15]	Errores en mantenimiento / Actualiza	Carencia de un plan de sustitucion de equipos	5
		[E.16]	Caida de sistema por agotamiento de	Falta de planes y procedimientos de continuidad de negocio	5
				Manejo inadecuado de la red	5
		[E.17]	Pérdida de equipos	Ausencia de personal	4
				Acceso no autorizado a las infraestructuras informáticas	4

		[A.4]	Abuso de privilegios de acceso	Atribución incorrecta de privilegios de acceso	3
		[A.5]	Uso no previsto	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Carencia de Politicas o reglamento interno	5
				Carencia de proteccion externa a las instalaciones	5
				Falta de control de acceso a oficinas o salones restringidos	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5
		[A.16]	Robo	Acceso físico no autorizado	5
				Falta de protección física del edificio, puertas y ventanas	4
		[A.17]	Ataque destructivo	Carencia de Politicas o reglamento interno	5
				Código malicioso	5
[servi.1]	Servidor de Backups	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Carencia de un plan de sustitucion de equipos	5
		[I.7]	Corte de suministro eléctrico	Susceptibilidad a las variaciones del voltaje	5
				Apagones por manipulacion de proveedor	4
		[I.8]	Condiciones inadecuadas	Ubicación de activos en espacios de riesgo	4
		[E.2]	Errores de administrador	Uso Incorrecto del hardware y software	4
				Falta de copias back-up	5
				Documentación de software incompleta o mal elaborada	4
		[E.4]	Errores de Configuración	Falta de manuales de configuración	5
		[E.6]	Disfusión de software dañino	Código malicioso	5
				Disposición o reutilización de los medios de almacenaje sin una apropiada verificación	3
				Falta de control de software ilegal o dañino	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[E.15]	Errores en mantenimiento / Actualiza	Carencia de un plan de sustitucion de equipos	5
		[E.16]	Caida de sistema por agotamiento de	Falta de planes y procedimientos de continuidad de negocio	5
				Manejo inadecuado de la red	5
		[E.17]	Pérdida de equipos	Ausencia de personal	4
				Acceso no autorizado a las infraestructuras informáticas	4
		[A.4]	Abuso de privilegios de acceso	Atribución incorrecta de privilegios de acceso	3

		[A.5]	Uso no previsto	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	5
				Carencia de Politicas o reglamento interno	5
				Carencia de proteccion externa a las instalaciones	5
				Falta de control de acceso a oficinas o salones restringidos	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5
		[A.16]	Robo	Acceso físico no autorizado	3
				Falta de protección física del edificio, puertas y ventanas	4
		[A.17]	Ataque destructivo	Carencia de Politicas o reglamento interno	5
				Código malicioso	5
[servi.2]	Servidor Myzro	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Carencia de un plan de sustitucion de equipos	5
		[I.7]	Corte de suministro eléctrico	Susceptibilidad a las variaciones del voltaje	5
				Apagones por manipulacion de proveedor	4
		[I.8]	Condiciones inadecuadas	Ubicación de activos en espacios de riesgo	4
		[E.2]	Errores de administrador	Uso Incorrecto del hardware y software	4
				Falta de copias back-up	5
				Documentación de software incompleta o mal elaborada	4
		[E.4]	Errores de Configuración	Falta de manuales de configuración	5
		[E.6]	Disfusión de software dañino	Código malicioso	5
				Disposición o reutilización de los medios de almacenaje sin una apropiada verificación	3
				Falta de control de software ilegal o dañino	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[E.15]	Errores en mantenimiento / Actualiza	Carencia de un plan de sustitucion de equipos	5
		[E.16]	Caida de sistema por agotamiento de	Falta de planes y procedimientos de continuidad de negocio	5
				Manejo inadecuado de la red	5
		[E.17]	Pérdida de equipos	Ausencia de personal	4
				Acceso no autorizado a las infraestructuras informáticas	4
		[A.4]	Abuso de privilegios de acceso	Atribución incorrecta de privilegios de acceso	3

		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Carencia de Politicas o reglamento interno	5
				Carencia de proteccion externa a las instalaciones	5
				Falta de control de acceso a oficinas o salones restringidos	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5
		[A.16]	Robo	Acceso físico no autorizado	4
				Falta de protección física del edificio, puertas y ventanas	4
		[A.17]	Ataque destructivo	Carencia de Politicas o reglamento interno	5
				Código malicioso	5
[switch]	Switches	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Carencia de un plan de sustitucion de equipos	5
		[I.7]	Corte de suministro eléctrico	Susceptibilidad a las variaciones del voltaje	5
				Apagones por manipulacion de proveedor	4
		[I.8]	Condiciones inadecuadas	Ubicación de activos en espacios de riesgo	4
		[E.2]	Errores de administrador	Uso Incorrecto del hardware y software	4
				Falta de copias back-up	5
				Documentación de software incompleta o mal elaborada	4
		[E.4]	Errores de Configuración	Falta de manuales de configuración	5
		[E.6]	Disfusión de software dañino	Código malicioso	5
				Disposición o reutilización de los medios de almacenaje sin una apropiada verificación	3
				Falta de control de software ilegal o dañino	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[E.15]	Errores en mantenimiento / Actualiza	Carencia de un plan de sustitucion de equipos	5
		[E.16]	Caida de sistema por agotamiento de	Falta de planes y procedimientos de continuidad de negocio	5
				Manejo inadecuado de la red	5
		[E.17]	Pérdida de equipos	Ausencia de personal	4
				Acceso no autorizado a las infraestructuras informáticas	4
		[A.4]	Abuso de privilegios de acceso	Atribución incorrecta de privilegios de acceso	3
		[A.5]	Uso no previsto	Descarga y uso incontrolado de software	4
				Manejo inadecuado de la red	5

		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Carencia de Politicas o reglamento interno	5
				Carencia de proteccion externa a las instalaciones	5
				Falta de control de acceso a oficinas o salones restringidos	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5
		[A.16]	Robo	Acceso físico no autorizado	4
				Falta de protección física del edificio, puertas y ventanas	4
		[A.17]	Ataque destructivo	Carencia de Politicas o reglamento interno	5
				Código malicioso	5
SI	**Soportes de Información**				
[san]	Almacenamiento en red	[E.1]	Errores de usuarios	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.10]	Alteración accidental de información	Uso Incorrecto del hardware y software	4
				Copiado incontrolado	4
		[A.5]	Uso no previsto	Descarga y uso incontrolado de software	4
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Carencia de Politicas o reglamento interno	5
				Carencia de proteccion externa a las instalaciones	5
				Falta de control de acceso a oficinas o salones restringidos	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
[cca]	Contratos, convenios, y acuerdo	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	Clima extremo	2
		[I.11]	Degradación de los soportes de alma	Falta de planes y procedimientos de continuidad de negocio	5
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[E.11]	Destruccion de información	Acceso físico no autorizado	4
				Dejar en sesión el sistema al salir del workstation.	4
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Carencia de Politicas o reglamento interno	5
		[A.10]	Modificación deliberada de informac	Atribución incorrecta de privilegios de acceso	3
				Falta de copias back-up	5

		[A.11]	Destrucción de información	Administración pobre de contraseñas	4
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	4
				Falta de políticas de contratación	4
		[A.16]	Robo	Acceso no autorizado a los ordenadores	4
				Ausencia de personal	4
				Instalaciones no protegidas	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de control de acceso a oficinas o salones restringidos	4
		[A.17]	Ataque destructivo	Carencia de Politicas o reglamento interno	5
				Código malicioso	5
[printed.1]	Diccionario de Datos	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	Clima extremo	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[E.6]	Disfusión de software dañino	Código malicioso	5
				Disposición o reutilización de los medios de almacenaje sin una apropiada verificación	3
				Falta de control de software ilegal o dañino	5
		[I.4]	Contaminación mecánica	Falta de planes de mantenimiento y limpieza de equipos	4
				Insuficiente mantenimiento / mala instalación de los medios de almacenaje.	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[I.11]	Degradación de los soportes de alma	Falta de planes y procedimientos de continuidad de negocio	5
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
		[E.12]	Fugas de información	Falta de planes y procedimientos de continuidad de negocio	5
				Administración pobre de contraseñas	4
				Falta de políticas de confidencialidad	5
		[A.5]	Uso no previsto	Descarga y uso incontrolado de software	4
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Carencia de Politicas o reglamento interno	5
		[A.10]	Modificación deliberada de informac	Atribución incorrecta de privilegios de acceso	3
				Falta de copias back-up	5
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4

		[A.16]	Robo	Acceso no autorizado a los ordenadores	4
				Ausencia de personal	4
				Instalaciones no protegidas	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de control de acceso a oficinas o salones restringidos	4
		[A.17]	Ataque destructivo	Carencia de Politicas o reglamento interno	5
				Código malicioso	5
[disk.2]	Disco Externo	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	Clima extremo	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[I.11]	Degradación de los soportes de alma	Falta de planes y procedimientos de continuidad de negocio	5
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
		[E.15]	Errores en mantenimiento / Actualiza	Carencia de un plan de sustitucion de equipos	5
		[E.17]	Pérdida de equipos	Ausencia de personal	4
				Acceso no autorizado a las infraestructuras informáticas	4
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Carencia de Politicas o reglamento interno	5
		[A.10]	Modificación deliberada de informac	Atribución incorrecta de privilegios de acceso	3
				Falta de copias back-up	5
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.14]	Manipulacion de Equipos	Falta políticas de uso de aplicaciones y de información	4
		[A.16]	Robo	Acceso no autorizado a los ordenadores	4
				Ausencia de personal	4
				Instalaciones no protegidas	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de control de acceso a oficinas o salones restringidos	4
		[A.17]	Ataque destructivo	Carencia de Politicas o reglamento interno	5
				Código malicioso	5

[printed.2]	Documentacion de los Sistemas	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	Clima extremo	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[E.2]	Errores de administrador	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
		[A.5]	Uso no previsto	Descarga y uso incontrolado de software	4
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Acceso no autorizado a la documentación del sistema	4
				Carencia de Politicas o reglamento interno	5
		[A.10]	Modificación deliberada de informac	Atribución incorrecta de privilegios de acceso	3
				Falta de copias back-up	5
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[A.16]	Robo	Acceso no autorizado a los ordenadores	4
				Ausencia de personal	4
				Instalaciones no protegidas	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de control de acceso a oficinas o salones restringidos	4

[printed.3]	Informes de Auditoria Médica	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	Clima extremo	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[I.11]	Degradación de los soportes de alma	Falta de planes y procedimientos de continuidad de negocio	5
		[E.2]	Errores de administrador	Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
				Uso Incorrecto del hardware y software	4
		[E.10]	Alteración accidental de información	Copiado incontrolado	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Acceso no autorizado a la documentación del sistema	4
				Carencia de Politicas o reglamento interno	5
		[A.10]	Modificación deliberada de informac	Atribución incorrecta de privilegios de acceso	3
				Falta de copias back-up	5
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[A.16]	Robo	Acceso no autorizado a los ordenadores	4
				Ausencia de personal	4
				Instalaciones no protegidas	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4

[usb]	USB Administrativos General	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	Fuga de agua	2
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	Clima extremo	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[E.11]	Destruccion de información	Código malicioso	5
				Falta de copias back-up	5
		[E.12]	Fugas de información	Falta de planes y procedimientos de continuidad de negocio	5
				Administración pobre de contraseñas	4
				Falta de políticas de confidencialidad	5
		[E.17]	Pérdida de equipos	Ausencia de personal	4
				Acceso no autorizado a las infraestructuras informáticas	4
		[A.10]	Modificación deliberada de informac	Atribución incorrecta de privilegios de acceso	3
				Falta de copias back-up	5
		[A.11]	Destrucción de información	Atribución incorrecta de privilegios de acceso	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[A.16]	Robo	Acceso no autorizado a los ordenadores	4
				Ausencia de personal	4
				Instalaciones no protegidas	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4

AUX	Equipamiento Auxiliar				
[ac]	Aires acondicionados	[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[E.15]	Errores en mantenimiento / Actualiza	Carencia de un plan de sustitucion de equipos	5
[power]	Fuentes de alimentación	[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[E.15]	Errores en mantenimiento / Actualiza	Carencia de un plan de sustitucion de equipos	5
[gen]	Generadores eléctricos	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[E.15]	Errores en mantenimiento / Actualiza	Carencia de un plan de sustitucion de equipos	5
[prp.5]	Sistema de control biometrico d	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[I.8]	Condiciones inadecuadas	Ubicación de activos en espacios de riesgo	4
		[I.10]	Interrupción de otros servicios y sumi	Falta de planes y procedimientos de continuidad de negocio	5
				Mala implementación de red	3
		[E.15]	Errores en mantenimiento / Actualiza	Atribución incorrecta de privilegios de acceso	3
		[E.17]	Pérdida de equipos	Carencia de un plan de sustitucion de equipos	5
				Falta de plan de sustitución de equipos	4
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Acceso no autorizado a la documentación del sistema	4
				Carencia de Politicas o reglamento interno	5
		[A.16]	Robo	Acceso no autorizado a los ordenadores	4
				Ausencia de personal	4
				Instalaciones no protegidas	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4

[furniture.1]	Stand Madera Oficinas	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[I.8]	Condiciones inadecuadas	Ubicación de activos en espacios de riesgo	4
		[I.10]	Interrupción de otros servicios y sumi	Falta de planes y procedimientos de continuidad de negocio	5
				Mala implementación de red	3
		[E.15]	Errores en mantenimiento / Actualiza	Atribución incorrecta de privilegios de acceso	3
		[E.17]	Pérdida de equipos	Carencia de un plan de sustitucion de equipos	5
				Falta de plan de sustitución de equipos	4
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Acceso no autorizado a la documentación del sistema	4
				Carencia de Politicas o reglamento interno	5
		[A.16]	Robo	Acceso no autorizado a los ordenadores	4
				Ausencia de personal	4
				Instalaciones no protegidas	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
[furniture.2]	Stand Metálica Oficinas	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[I.8]	Condiciones inadecuadas	Ubicación de activos en espacios de riesgo	4
		[E.15]	Errores en mantenimiento / Actualiza	Atribución incorrecta de privilegios de acceso	3
		[E.17]	Pérdida de equipos	Carencia de un plan de sustitucion de equipos	5
				Falta de plan de sustitución de equipos	4
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Acceso no autorizado a la documentación del sistema	4
				Carencia de Politicas o reglamento interno	5
		[A.16]	Robo	Acceso no autorizado a los ordenadores	4
				Ausencia de personal	4
				Instalaciones no protegidas	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4

[ups]	UPS Informática	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
		[N.3]	Desastres Naturales	Clima extremo	2
		[I.4]	Contaminación mecánica	Susceptibilidad a la humedad, al polvo	5
				Falta de planes de mantenimiento y limpieza de equipos	4
		[I.6]	Averías de origen físico o lógico	Falta de planes de mantenimiento y limpieza de equipos	4
		[I.8]	Condiciones inadecuadas	Ubicación de activos en espacios de riesgo	4
		[I.10]	Interrupción de otros servicios y sumi	Falta de planes y procedimientos de continuidad de negocio	5
				Mala implementación de red	3
		[E.15]	Errores en mantenimiento / Actualiza	Atribución incorrecta de privilegios de acceso	3
		[E.17]	Pérdida de equipos	Carencia de un plan de sustitucion de equipos	5
				Falta de plan de sustitución de equipos	4
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Acceso no autorizado a la documentación del sistema	4
				Carencia de Politicas o reglamento interno	5
		[A.16]	Robo	Acceso no autorizado a los ordenadores	4
				Ausencia de personal	4
				Instalaciones no protegidas	4
				Uso inadecuado o descuidado del control de acceso físico al edificio	4
		[A.17]	Ataque destructivo	Carencia de Politicas o reglamento interno	5
				Código malicioso	5
COM	Redes de Comunicaciones				
[WAN]	Red de área amplia	[I.9]	Falla de servicios de comunicaciones	Conexiones de red pública desprotegidas	4
				Fallo del sistema	5
				Insuficiente mantenimiento / mala instalación de los medios de almacenaje.	4
		[E.2]	Errores de administrador	Mala implementación de red	3
				Conexiones de red pública desprotegidas	4
		[E.7]	Errores de reencaminamiento	Falta de identificación y autentificación del remitente y del receptor	4
				Falta de políticas para el uso correcto de los medios de telecomunicación y mensajería	4
		[E.8]	Errores de secuencia	Falta de pruebas de envío y recibimiento del mensaje	4
		[E.10]	Alteración accidental de información	Manejo inadecuado de la red	5
		[E.11]	Destruccion de información	Código malicioso	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.9]	Intercepción de información	Falta de planes y procedimientos de continuidad de negocio	5
				Conexiones de red pública desprotegidas	4

		[A.10]	Modificación deliberada de informac	Mala implementación de red	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5
[LAN]	Red local	[I.9]	Falla de servicios de comunicaciones	Conexiones de red pública desprotegidas	4
				Fallo del sistema	5
				Insuficiente mantenimiento / mala instalación de los medios de almacenaje.	4
		[E.2]	Errores de administrador	Mala implementación de red	3
				Conexiones de red pública desprotegidas	4
		[E.7]	Errores de reencaminamiento	Falta de identificación y autentificación del remitente y del receptor	4
				Falta de políticas para el uso correcto de los medios de telecomunicación y mensajería	4
		[E.8]	Errores de secuencia	Falta de pruebas de envío y recibimiento del mensaje	4
		[E.10]	Alteración accidental de información	Manejo inadecuado de la red	5
		[E.11]	Destruccion de información	Código malicioso	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.9]	Intercepción de información	Falta de planes y procedimientos de continuidad de negocio	5
				Conexiones de red pública desprotegidas	4
		[A.10]	Modificación deliberada de informac	Mala implementación de red	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5
[PSTN]	Red telefónica	[I.9]	Falla de servicios de comunicaciones	Conexiones de red pública desprotegidas	4
				Fallo del sistema	5
				Insuficiente mantenimiento / mala instalación de los medios de almacenaje.	4
		[E.2]	Errores de administrador	Mala implementación de red	3
				Conexiones de red pública desprotegidas	4
		[E.7]	Errores de reencaminamiento	Falta de identificación y autentificación del remitente y del receptor	4
				Falta de políticas para el uso correcto de los medios de telecomunicación y mensajería	4
		[E.8]	Errores de secuencia	Falta de pruebas de envío y recibimiento del mensaje	4
		[E.10]	Alteración accidental de información	Manejo inadecuado de la red	5
		[E.11]	Destruccion de información	Código malicioso	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.9]	Intercepción de información	Falta de planes y procedimientos de continuidad de negocio	5
				Conexiones de red pública desprotegidas	4
		[A.10]	Modificación deliberada de informac	Mala implementación de red	3

		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5
[wifi]	Wifi	[I.9]	Falla de servicios de comunicaciones	Conexiones de red pública desprotegidas	4
				Fallo del sistema	5
				Insuficiente mantenimiento / mala instalación de los medios de almacenaje.	4
		[E.2]	Errores de administrador	Mala implementación de red	3
				Conexiones de red pública desprotegidas	4
		[E.7]	Errores de reencaminamiento	Falta de identificación y autentificación del remitente y del receptor	4
				Falta de políticas para el uso correcto de los medios de telecomunicación y mensajería	4
		[E.8]	Errores de secuencia	Falta de pruebas de envío y recibimiento del mensaje	4
		[E.10]	Alteración accidental de información	Manejo inadecuado de la red	5
		[E.11]	Destruccion de información	Código malicioso	5
		[E.12]	Fugas de información	Falta de políticas de confidencialidad	5
		[A.9]	Intercepción de información	Falta de planes y procedimientos de continuidad de negocio	5
				Conexiones de red pública desprotegidas	4
		[A.10]	Modificación deliberada de informac	Mala implementación de red	3
		[A.12]	Divulgación de información	Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
		[A.15]	Denegacion de Servicio	Manejo inadecuado de la red	5
L	Instalaciones				
[building.1]	Edificio Clinica	[N.1]	Daños por fuego	Ubicación de activos en espacios de riesgo	4
				No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	No planes de contingencia en caso de desastres	5
				Ubicación de activos en espacios de riesgo	4
				Nivel inapropiado de protección criptográfica	4
		[E.10]	Alteración accidental de información	Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de capacitacion del personal en seguridad	5
		[E.11]	Destruccion de información	Instalaciones no protegidas	4
				Falta de recursos de proteccion de TI	5
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Falta de protección física del edificio, puertas y ventanas	4

		[A.17]	Ataque destructivo	Falta de mecanismos de monitoreo	3
				Carencia de Politicas o reglamento interno	5
		[A.18]	Ocupación enemiga	Falta de control de acceso a oficinas o salones restringidos	4
[building.2]	Edificio Torre Nueva	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	No planes de contingencia en caso de desastres	5
		[E.10]	Alteración accidental de información	Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de capacitacion del personal en seguridad	5
		[E.11]	Destruccion de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
				Instalaciones no protegidas	4
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Nivel inapropiado de protección criptográfica	4
				Falta de protección física del edificio, puertas y ventanas	4
		[A.17]	Ataque destructivo	Falta de mecanismos de monitoreo	3
				Carencia de Politicas o reglamento interno	5
		[A.18]	Ocupación enemiga	Falta de control de acceso a oficinas o salones restringidos	4
[local.1]	Oficinas 1 piso	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	No planes de contingencia en caso de desastres	5
		[E.10]	Alteración accidental de información	Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de capacitacion del personal en seguridad	5
		[E.11]	Destruccion de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
				Instalaciones no protegidas	4
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Nivel inapropiado de protección criptográfica	4
				Falta de protección física del edificio, puertas y ventanas	4
		[A.10]	Modificación deliberada de informac	Acceso físico no autorizado	4
				Administración pobre de contraseñas	4
				Carencia de Politicas o reglamento interno	5
		[A.11]	Destrucción de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5

		[A.12]	Divulgación de información	Instalaciones no protegidas	4
		[A.17]	Ataque destructivo	Falta de mecanismos de monitoreo	3
				Carencia de Politicas o reglamento interno	5
		[A.18]	Ocupación enemiga	Falta de control de acceso a oficinas o salones restringidos	4
[local.2]	Oficinas 2 piso	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	No planes de contingencia en caso de desastres	5
		[E.10]	Alteración accidental de información	Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de capacitacion del personal en seguridad	5
		[E.11]	Destruccion de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
				Instalaciones no protegidas	4
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Nivel inapropiado de protección criptográfica	4
				Falta de protección física del edificio, puertas y ventanas	4
		[A.10]	Modificación deliberada de informac	Acceso físico no autorizado	4
				Administración pobre de contraseñas	4
				Carencia de Politicas o reglamento interno	5
		[A.11]	Destrucción de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
		[A.12]	Divulgación de información	Instalaciones no protegidas	4
		[A.17]	Ataque destructivo	Falta de mecanismos de monitoreo	3
				Carencia de Politicas o reglamento interno	5
		[A.18]	Ocupación enemiga	Falta de control de acceso a oficinas o salones restringidos	4
[local.3]	Oficinas 3 piso	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	No planes de contingencia en caso de desastres	5
		[E.10]	Alteración accidental de información	Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de capacitacion del personal en seguridad	5
		[E.11]	Destruccion de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
				Instalaciones no protegidas	4
				Falta de planes y procedimientos de continuidad de negocio	5

		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Nivel inapropiado de protección criptográfica	4
				Falta de protección física del edificio, puertas y ventanas	4
		[A.10]	Modificación deliberada de informac	Acceso físico no autorizado	4
				Administración pobre de contraseñas	4
				Carencia de Politicas o reglamento interno	5
		[A.11]	Destrucción de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
		[A.12]	Divulgación de información	Instalaciones no protegidas	4
		[A.17]	Ataque destructivo	Falta de mecanismos de monitoreo	3
				Carencia de Politicas o reglamento interno	5
		[A.18]	Ocupación enemiga	Falta de control de acceso a oficinas o salones restringidos	4
[local.4]	Sector Consultorios Medicos Clinica	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	No planes de contingencia en caso de desastres	5
		[E.10]	Alteración accidental de información	Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de capacitacion del personal en seguridad	5
		[E.11]	Destruccion de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
				Instalaciones no protegidas	4
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Nivel inapropiado de protección criptográfica	4
				Falta de protección física del edificio, puertas y ventanas	4
		[A.10]	Modificación deliberada de informac	Acceso físico no autorizado	4
				Administración pobre de contraseñas	4
				Carencia de Politicas o reglamento interno	5
		[A.11]	Destrucción de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
		[A.12]	Divulgación de información	Instalaciones no protegidas	4
		[A.17]	Ataque destructivo	Falta de mecanismos de monitoreo	3
				Carencia de Politicas o reglamento interno	5
		[A.18]	Ocupación enemiga	Falta de control de acceso a oficinas o salones restringidos	4

[local.5]	Sector Consultorios Medicos Torre Nueva	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	No planes de contingencia en caso de desastres	5
		[E.10]	Alteración accidental de información	Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de capacitacion del personal en seguridad	5
		[E.11]	Destruccion de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
				Instalaciones no protegidas	4
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Nivel inapropiado de protección criptográfica	4
				Falta de protección física del edificio, puertas y ventanas	4
		[A.10]	Modificación deliberada de informac	Acceso físico no autorizado	4
				Administración pobre de contraseñas	4
				Carencia de Politicas o reglamento interno	5
		[A.11]	Destrucción de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
		[A.12]	Divulgación de información	Instalaciones no protegidas	4
		[A.17]	Ataque destructivo	Falta de mecanismos de monitoreo	3
				Carencia de Politicas o reglamento interno	5
		[A.18]	Ocupación enemiga	Falta de control de acceso a oficinas o salones restringidos	4
[local.6]	Sector Historias Clinicas	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	No planes de contingencia en caso de desastres	5
		[E.10]	Alteración accidental de información	Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de capacitacion del personal en seguridad	5
		[E.11]	Destruccion de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
				Instalaciones no protegidas	4
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Nivel inapropiado de protección criptográfica	4
				Falta de protección física del edificio, puertas y ventanas	4

		[A.10]	Modificación deliberada de informac	Acceso físico no autorizado	4
				Administración pobre de contraseñas	4
				Carencia de Politicas o reglamento interno	5
		[A.11]	Destrucción de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
		[A.12]	Divulgación de información	Instalaciones no protegidas	4
		[A.17]	Ataque destructivo	Falta de mecanismos de monitoreo	3
				Carencia de Politicas o reglamento interno	5
		[A.18]	Ocupación enemiga	Falta de control de acceso a oficinas o salones restringidos	4
[local.7]	Sector Informatica	[N.1]	Daños por fuego	No planes de contingencia en caso de desastres	5
		[N.2]	Daños por agua	No planes de contingencia en caso de desastres	5
				Localización en un área susceptible a la inundación	2
		[N.3]	Desastres Naturales	No planes de contingencia en caso de desastres	5
		[E.10]	Alteración accidental de información	Uso inadecuado o descuidado del control de acceso físico al edificio	4
				Falta de capacitacion del personal en seguridad	5
		[E.11]	Destruccion de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
				Instalaciones no protegidas	4
				Falta de planes y procedimientos de continuidad de negocio	5
		[A.7]	Acceso no autorizado	Acceso físico no autorizado	4
				Nivel inapropiado de protección criptográfica	4
				Falta de protección física del edificio, puertas y ventanas	4
		[A.10]	Modificación deliberada de informac	Acceso físico no autorizado	4
				Administración pobre de contraseñas	4
				Carencia de Politicas o reglamento interno	5
		[A.11]	Destrucción de información	Ubicación de activos en espacios de riesgo	4
				Falta de recursos de proteccion de TI	5
		[A.12]	Divulgación de información	Instalaciones no protegidas	4
		[A.17]	Ataque destructivo	Falta de mecanismos de monitoreo	3
				Carencia de Politicas o reglamento interno	5
		[A.18]	Ocupación enemiga	Falta de control de acceso a oficinas o salones restringidos	4

P	Personal				
[ui.1]	Administrativos General	[E.5]	Deficiencias de la organización	Carencia de Politicas o reglamento interno	5
				Protección de la información de la organización	4
				Responsabilidades no claramente definidas	4
		[E.12]	Fugas de información	Administración pobre de contraseñas	5
				Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
				Empleados desmotivados	4
				Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
		[E.18]	Indisponibilidad del personal	Falta de sensibilización	4
		[A.19]	Indisponibilidad del personal	Falta políticas de uso de aplicaciones y de información	4
		[A.20]	Extorsion	Confianza de las organizaciones clave hacia la compañía.	2
		[A.21]	Ingenieria social	Confianza de las organizaciones clave hacia la compañía.	2
[ui.2]	Gerencia Administrativa	[E.5]	Deficiencias de la organización	Carencia de Politicas o reglamento interno	5
				Protección de la información de la organización	4
				Responsabilidades no claramente definidas	4
		[E.12]	Fugas de información	Administración pobre de contraseñas	5
				Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
				Empleados desmotivados	4
				Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
		[E.18]	Indisponibilidad del personal	Falta de sensibilización	4
		[A.19]	Indisponibilidad del personal	Falta políticas de uso de aplicaciones y de información	4
		[A.20]	Extorsion	Confianza de las organizaciones clave hacia la compañía.	2
		[A.21]	Ingenieria social	Confianza de las organizaciones clave hacia la compañía.	2

[ui.3]	Jefaturas	[E.5]	Deficiencias de la organización	Carencia de Politicas o reglamento interno	5
				Protección de la información de la organización	4
				Responsabilidades no claramente definidas	4
		[E.12]	Fugas de información	Administración pobre de contraseñas	5
				Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
				Empleados desmotivados	4
				Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
		[E.18]	Indisponibilidad del personal	Falta de sensibilización	4
		[A.19]	Indisponibilidad del personal	Falta políticas de uso de aplicaciones y de información	4
		[A.20]	Extorsion	Confianza de las organizaciones clave hacia la compañía.	2
		[A.21]	Ingenieria social	Confianza de las organizaciones clave hacia la compañía.	2
[adm]	Administradores de sistemas	[E.5]	Deficiencias de la organización	Carencia de Politicas o reglamento interno	5
				Protección de la información de la organización	4
				Responsabilidades no claramente definidas	4
		[E.12]	Fugas de información	Administración pobre de contraseñas	5
				Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
				Empleados desmotivados	4
				Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
		[E.18]	Indisponibilidad del personal	Falta de sensibilización	4
		[A.19]	Indisponibilidad del personal	Falta políticas de uso de aplicaciones y de información	4
		[A.20]	Extorsion	Confianza de las organizaciones clave hacia la compañía.	2
		[A.21]	Ingenieria social	Confianza de las organizaciones clave hacia la compañía.	2

[des]	Desarrolladores/ programadores	[E.5]	Deficiencias de la organización	Carencia de Politicas o reglamento interno	5
				Protección de la información de la organización	4
				Responsabilidades no claramente definidas	4
		[E.12]	Fugas de información	Administración pobre de contraseñas	5
				Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
				Empleados desmotivados	4
				Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
		[E.18]	Indisponibilidad del personal	Falta de sensibilización	4
		[A.19]	Indisponibilidad del personal	Falta políticas de uso de aplicaciones y de información	4
		[A.20]	Extorsion	Confianza de las organizaciones clave hacia la compañía.	2
		[A.21]	Ingenieria social	Confianza de las organizaciones clave hacia la compañía.	2
[ui.4]	Personal Asistencial, Ténicos y Laboratoristas	[E.5]	Deficiencias de la organización	Carencia de Politicas o reglamento interno	5
				Protección de la información de la organización	4
				Responsabilidades no claramente definidas	4
		[E.12]	Fugas de información	Administración pobre de contraseñas	5
				Falta de políticas de confidencialidad	5
				Falta de políticas de contratación	4
				Empleados desmotivados	4
				Falta de capacitacion del personal en seguridad	5
				Falta de capacitación del personal en uso de aplicaciones	5
		[E.18]	Indisponibilidad del personal	Falta de sensibilización	4
		[A.19]	Indisponibilidad del personal	Falta políticas de uso de aplicaciones y de información	4
		[A.20]	Extorsion	Confianza de las organizaciones clave hacia la compañía.	2
		[A.21]	Ingenieria social	Confianza de las organizaciones clave hacia la compañía.	2

[ui.5]	Personal de Auditoria Medica	[E.5]	Deficiencias de la organización	Carencia de Politicas o reglamento interno	5	
				Protección de la información de la organización	4	
				Responsabilidades no claramente definidas	4	
		[E.12]	Fugas de información	Administración pobre de contraseñas	5	
				Falta de políticas de confidencialidad	5	
				Falta de políticas de contratación	4	
				Empleados desmotivados	4	
				Falta de capacitacion del personal en seguridad	5	
				Falta de capacitación del personal en uso de aplicaciones	5	
		[E.18]	Indisponibilidad del personal	Falta de sensibilización	4	
		[A.19]	Indisponibilidad del personal	Falta políticas de uso de aplicaciones y de información	4	
		[A.20]	Extorsion	Confianza de las organizaciones clave hacia la compañía.	2	
		[A.21]	Ingenieria social	Confianza de las organizaciones clave hacia la compañía.	2	
[ui.6]	Personal Hist Clinicas	[E.5]	Deficiencias de la organización	Carencia de Politicas o reglamento interno	5	
				Protección de la información de la organización	4	
				Responsabilidades no claramente definidas	4	
		[E.12]	Fugas de información	Administración pobre de contraseñas	5	
				Falta de políticas de confidencialidad	5	
				Falta de políticas de contratación	4	
				Empleados desmotivados	4	
				Falta de capacitacion del personal en seguridad	5	
				Falta de capacitación del personal en uso de aplicaciones	5	
		[E.18]	Indisponibilidad del personal	Falta de sensibilización	4	
		[A.19]	Indisponibilidad del personal	Falta políticas de uso de aplicaciones y de información	4	
		[A.20]	Extorsion	Confianza de las organizaciones clave hacia la compañía.	2	
		[A.21]	Ingenieria social	Confianza de las organizaciones clave hacia la compañía.	2	

- **Caracterización de Salvaguardas**

VALORACION DE SALVAGUARDAS				
Eficacia : ¿Cuán eficaz es la salvaguarda?				[E]
¿De qué manera la perdida del activo afecta la C.I.D.?				
ACTIVOS POR TIPO		SALVAGUARDA Y/O CONTROL	TIPO	E
D	Datos/Información			
[bd.1]	Base de Datos Atenciones	Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Cifrado de la información	Administrativas	10%
		Se aplican perfiles de seguridad	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[bd.2]	Base de Datos General	Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Cifrado de la información	Administrativas	10%
		Se aplican perfiles de seguridad	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[bd.3]	Base de Datos Myzro	Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Cifrado de la información	Administrativas	10%
		Se aplican perfiles de seguridad	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[bd.4]	Base de Datos Kardex	Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Cifrado de la información	Administrativas	10%
		Se aplican perfiles de seguridad	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[exe]	Codigo ejecutable	Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
[source.1]	Codigo Fuente Atenciones	Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Se aplican perfiles de seguridad	Preventiva	40%
		Cifrado de la información	Administrativas	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[source.2]	Codigo Fuente Myzro	Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Cifrado de la información	Administrativas	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[source.3]	Codigo Fuente Ventas	Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Cifrado de la información	Administrativas	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%

[backup]	Copias de respaldo	Politicas ligadas a los recursos humanos	Concienciación	10%
[password]	Credenciales (contraseñas)	Se aplican perfiles de seguridad	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[conf]	Datos de configuración	Politicas ligadas a los recursos humanos	Concienciación	10%
[acl]	Datos de control de acceso	Identificación y autenticación	Preventiva	10%
		Se aplican perfiles de seguridad	Preventiva	40%
[test]	Datos de prueba	Politicas ligadas a los recursos humanos	Concienciación	10%
		Identificación y autenticación	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[files]	Ficheros	Politicas ligadas a los recursos humanos	Concienciación	10%
		Identificación y autenticación	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[hc]	Historias Clinicas	Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Cifrado de la información	Administrativas	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Identificación y autenticación	Preventiva	10%
S	Servicios			
[file]	Almacenamiento de ficheros	Identificación y autenticación	Preventiva	10%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Identificación y autenticación	Preventiva	10%
		Control de acceso lógico	Preventiva	10%
[email]	Correo electrónico Institucion	Protección del directorio	Preventiva	10%
		Se aplican perfiles de seguridad	Preventiva	40%
[www]	Internet	Protección del servidor de nombres de dominio (DNS)	Preventiva	40%
[cont]	Proveedores de T.I	Control de acceso lógico	Preventiva	40%
		Identificación y autenticación	Preventiva	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[s.back]	Servicio de copias de respald	Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[dns]	Servidor de nombres de domi	Identificación y autenticación	Preventiva	10%
		Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
[voip]	Telefonía IP	Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
SW	Aplicaciones/Software			
[browser.1]	Google Chrome	Control de acceso lógico	Preventiva	40%
[browser.2]	Internet Explorer	Control de acceso lógico	Preventiva	40%
[av]	Mcafee	Cambios (actualizaciones y mantenimiento)	Preventiva	10%
[office]	Microsof Office	Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Se aplican perfiles de seguridad	Preventiva	40%
[dbms.1]	MySQL	Copias de seguridad de los datos (backup)	Preventiva	40%
		Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Identificación y autenticación	Preventiva	10%

[dbms.2]	Oracle	Copias de seguridad de los datos (backup)	Preventiva	40%
		Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
[prp.1]	Sistema Atenciones	Control de acceso lógico	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
[a.back]	Sistema de backup	Control de acceso lógico	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
[prp.2]	Sistema Myzro	Control de acceso lógico	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
[prp.3]	Sistema Ventas	Control de acceso lógico	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
[prp.4]	Sistemas General	Control de acceso lógico	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
[dbms.3]	SQL Server 2008	Copias de seguridad de los datos (backup)	Preventiva	40%
		Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
[windows.1]	Windows 7	Control de acceso lógico	Preventiva	40%
		Aplicaciones: Adquisición o desarrollo	Preventiva	10%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[windows.2]	Windows XP	Control de acceso lógico	Preventiva	40%
		Aplicaciones: Adquisición o desarrollo	Preventiva	10%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
HW	Equipos Informáticos			
[print]	Impresora	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Climatización	Preventiva	10%
		Instalación	Preventiva	40%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
[pc.1]	PC Administrativos General	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Aplicaciones: Adquisición o desarrollo	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas de Clasificación de la información.	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
[pc.2]	PC Clinica	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Aplicaciones: Adquisición o desarrollo	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas de Clasificación de la información.	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%

[pc.3]	PC Gerencia Administrativa	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Aplicaciones: Adquisición o desarrollo	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas de Clasificación de la información.	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
[pc.4]	PC Informática	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Aplicaciones: Adquisición o desarrollo	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas de Clasificación de la información.	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
[pc.5]	PC Jefaturas	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Aplicaciones: Adquisición o desarrollo	Preventiva	10%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas de Clasificación de la información.	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
[scan]	Scanner	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Climatización	Preventiva	10%
		Instalación	Preventiva	40%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
[pabx]	Servidor Central Telefónica	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Instalación	Preventiva	40%
		Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Control de acceso lógico	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Control de acceso lógico	Preventiva	40%
		Se aplican perfiles de seguridad	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%

[servi.1]	Servidor de Backups	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Instalación	Preventiva	40%
		Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Control de acceso lógico	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Control de acceso lógico	Preventiva	40%
		Se aplican perfiles de seguridad	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
[servi.2]	Servidor Myzro	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Instalación	Preventiva	40%
		Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Control de acceso lógico	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Control de acceso lógico	Preventiva	40%
		Se aplican perfiles de seguridad	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
[switch]	Switches	Protección de las Instalaciones	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Suministro eléctrico	Preventiva	10%
		Instalación	Preventiva	40%
		Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Control de acceso lógico	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
SI	**Soportes de Información**			
[san]	Almacenamiento en red	Control de los accesos físicos	Preventiva	10%
[cca]	Contratos, convenios, y acuerd	Copias de seguridad de los datos (backup)	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Control de los accesos físicos	Preventiva	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Identificación y autenticación	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%

[printed.1]	Diccionario de Datos	Protección de las Instalaciones	Preventiva	40%
		Control de acceso lógico	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Control de los accesos físicos	Preventiva	10%
[disk.2]	Disco Externo	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Control de acceso lógico	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Control de los accesos físicos	Preventiva	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
[printed.2]	Documentacion de los Sistem	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Control de acceso lógico	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Control de acceso lógico	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Control de los accesos físicos	Preventiva	10%
[printed.3]	Informes de Auditoria Médica	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Control de acceso lógico	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Control de acceso lógico	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Control de los accesos físicos	Preventiva	10%
[usb]	USB Administrativos General	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Control de acceso lógico	Preventiva	40%
		Identificación y autenticación	Preventiva	10%
		Politicas de Responsabilidades y procedimientos de operación	Administrativas	10%
		Se aplican perfiles de seguridad	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
		Control de los accesos físicos	Preventiva	10%
AUX	**Equipamiento Auxiliar**			
[ac]	Aires acondicionados	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%

[power]	Fuentes de alimentación	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
[gen]	Generadores eléctricos	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
[prp.5]	Sistema de control biometrico	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Instalación	Preventiva	40%
		Se aplican perfiles de seguridad	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
[furniture.1]	Stand Madera Oficinas	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Instalación	Preventiva	40%
		Se aplican perfiles de seguridad	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
[furniture.2]	Stand Metálica Oficinas	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Instalación	Preventiva	40%
		Se aplican perfiles de seguridad	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
[ups]	UPS Informática	Protección de las Instalaciones	Preventiva	40%
		Copias de seguridad de los datos (backup)	Preventiva	40%
		Instalación	Preventiva	40%
		Se aplican perfiles de seguridad	Preventiva	40%
		Cambios (actualizaciones y mantenimiento)	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
COM	**Redes de Comunicaciones**			
[WAN]	Red de área amplia	Protección del cableado	Preventiva	10%
		Control de acceso lógico	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[LAN]	Red local	Protección del cableado	Preventiva	10%
		Control de acceso lógico	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[PSTN]	Red telefónica	Protección del cableado	Preventiva	10%
		Control de acceso lógico	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%
[wifi]	Wifi	Protección del cableado	Preventiva	10%
		Control de acceso lógico	Preventiva	40%
		Politicas ligadas a los recursos humanos	Concienciación	10%

L	Instalaciones			
[building.1]	Edificio Clinica	Instalación	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
[building.2]	Edificio Torre Nueva	Instalación	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
[local.1]	Oficinas 1 piso	Instalación	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
[local.2]	Oficinas 2 piso	Instalación	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
[local.3]	Oficinas 3 piso	Instalación	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
[local.4]	Sector Consultorios Medicos Clinica	Instalación	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
[local.5]	Sector Consultorios Medicos Torre Nueva	Instalación	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
[local.6]	Sector Historias Clinicas	Instalación	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
[local.7]	Sector Informatica	Instalación	Preventiva	40%
		Control de los accesos físicos	Preventiva	10%
		Politicas de Seguridad Física	Preventiva	10%
		Control de los accesos físicos	Preventiva	10%
		Identificación y autenticación	Preventiva	10%

P	Personal			
[ui.1]	Administrativos General	Politicas de Seguridad Física	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Monitorización	10%
[ui.2]	Gerencia Administrativa	Politicas de Seguridad Física	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Monitorización	10%
[ui.3]	Jefaturas	Politicas de Seguridad Física	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Monitorización	10%
[adm]	Administradores de sistemas	Politicas de Seguridad Física	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Monitorización	10%
[des]	Desarrolladores/programador	Politicas de Seguridad Física	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Monitorización	10%
[ui.4]	Personal Asistencial, Ténicos	Politicas de Seguridad Física	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Monitorización	10%
[ui.5]	Personal de Auditoria Medica	Politicas de Seguridad Física	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Monitorización	10%
[ui.6]	Personal Hist Clinicas	Politicas de Seguridad Física	Preventiva	10%
		Identificación y autenticación	Preventiva	10%
		Control de los accesos físicos	Monitorización	10%

- **En este punto se ve el impacto potencial y el impacto residual**

DETERMINACION DE IMPACTO POTENCIAL Y RESIDUAL								
Probabilidad residual de Ocurrencia de una amenza sobre un activo : ¿Cuán probable o improbable es que se materialice la								[PR]
La degradacion residual de la amenaza sobre el activo : ¿Cuán perjudicado resultaría el [valor del] activo con salvaguardas								[DR]
Impacto Residual [IR]¿ Cual es la Medida del daño que causa sobre el activo la materialización de una amenaza?								
ACTIVOS POR TIPO		**AMENAZAS**		**PR**	**DR**	**IP**	**IR**	
D	**Datos/Información**							
[bd.1]	Base de Datos Atenciones	[E.2]	Errores de administrador	5	90%	5	5	
		[E.4]	Errores de Configuración	4	80%	4	3	
		[E.10]	Alteración accidental de información	3	60%	4	2	
		[E.11]	Destruccion de información	5	100%	5	5	
		[A.7]	Acceso no autorizado	5	90%	5	5	
		[A.11]	Destrucción de información	5	90%	5	5	
		[A.12]	Divulgación de información	5	90%	5	5	
[bd.2]	Base de Datos General	[E.2]	Errores de administrador	5	90%	4	4	
		[E.4]	Errores de Configuración	4	80%	3	3	
		[E.10]	Alteración accidental de información	3	60%	3	2	
		[E.11]	Destruccion de información	5	100%	4	4	
		[A.7]	Acceso no autorizado	5	90%	4	4	
		[A.11]	Destrucción de información	5	90%	4	4	
		[A.12]	Divulgación de información	5	90%	4	4	
[bd.3]	Base de Datos Myzro	[E.2]	Errores de administrador	5	90%	4	3	
		[E.4]	Errores de Configuración	4	80%	4	3	
		[E.10]	Alteración accidental de información	3	60%	4	2	
		[E.11]	Destruccion de información	5	100%	5	5	
		[A.7]	Acceso no autorizado	5	90%	5	4	
		[A.11]	Destrucción de información	5	90%	5	4	
		[A.12]	Divulgación de información	5	90%	5	4	
[bd.4]	Base de Datos Kardex	[E.2]	Errores de administrador	5	90%	5	5	
		[E.4]	Errores de Configuración	4	80%	4	3	
		[E.10]	Alteración accidental de información	2	60%	4	2	
		[E.11]	Destruccion de información	3	100%	5	5	
		[A.7]	Acceso no autorizado	4	90%	5	5	
		[A.11]	Destrucción de información	5	90%	5	5	
		[A.12]	Divulgación de información	4	90%	5	5	
[exe]	Codigo ejecutable	[E.2]	Errores de administrador	5	90%	3	3	
		[E.3]	Errores de Monitorización	5	100%	4	4	
		[E.11]	Destruccion de información	5	100%	4	4	
[source.1]	Codigo Fuente Atenciones	[E.2]	Errores de administrador	5	90%	4	4	
		[E.4]	Errores de Configuración	4	80%	3	3	
		[E.10]	Alteración accidental de información	2	60%	3	2	
		[E.11]	Destruccion de información	4	100%	4	4	
		[A.7]	Acceso no autorizado	4	75%	4	3	
		[A.11]	Destrucción de información	3	60%	4	3	
		[A.12]	Divulgación de información	5	90%	4	4	

[source.2]	Codigo Fuente Myzro	[E.2]	Errores de administrador	5	90%	5	4
		[E.4]	Errores de Configuración	4	80%	4	3
		[E.10]	Alteración accidental de información	3	60%	4	2
		[E.11]	Destruccion de información	4	100%	5	5
		[A.7]	Acceso no autorizado	3	75%	5	4
		[A.11]	Destrucción de información	3	60%	5	3
		[A.12]	Divulgación de información	5	90%	5	4
[source.3]	Codigo Fuente Ventas	[E.2]	Errores de administrador	4	90%	4	4
		[E.4]	Errores de Configuración	5	100%	4	4
		[E.10]	Alteración accidental de información	2	60%	3	2
		[E.11]	Destruccion de información	4	100%	4	4
		[A.7]	Acceso no autorizado	4	75%	3	3
		[A.11]	Destrucción de información	2	60%	4	3
		[A.12]	Divulgación de información	4	90%	4	4
[backup]	Copias de respaldo	[E.11]	Destruccion de información	5	100%	5	5
		[E.12]	Fugas de información	4	90%	4	3
		[A.11]	Destrucción de información	4	100%	5	5
[password]	Credenciales (contraseñas)	[E.11]	Destruccion de información	3	60%	4	2
		[E.12]	Fugas de información	4	90%	3	3
		[A.11]	Destrucción de información	4	100%	4	4
[conf]	Datos de configuración	[E.4]	Errores de Configuración	4	80%	3	2
		[E.11]	Destruccion de información	5	90%	3	3
		[E.12]	Fugas de información	4	80%	3	2
		[A.11]	Destrucción de información	5	100%	3	3
[acl]	Datos de control de acceso	[E.11]	Destruccion de información	5	90%	5	5
		[E.12]	Fugas de información	3	80%	4	3
		[A.11]	Destrucción de información	2	60%	5	3
[test]	Datos de prueba	[E.11]	Destruccion de información	5	90%	3	3
		[E.12]	Fugas de información	3	80%	2	2
		[A.11]	Destrucción de información	4	90%	3	3
[files]	Ficheros	[E.11]	Destruccion de información	5	90%	4	4
		[E.12]	Fugas de información	3	80%	3	3
		[A.1]	Manipulación de los registros de actividad (log	3	100%	4	4
		[A.11]	Destrucción de información	4	90%	4	4
[hc]	Historias Clinicas	[E.11]	Destruccion de información	5	90%	5	4
		[E.12]	Fugas de información	3	80%	4	3
		[A.7]	Acceso no autorizado	3	90%	4	3
		[A.11]	Destrucción de información	5	90%	5	4
S	Servicios						
[file]	Almacenamiento de ficheros	[E.11]	Destruccion de información	3	75%	5	4
		[E.12]	Fugas de información	4	90%	5	5
		[A.7]	Acceso no autorizado	5	90%	4	4
		[A.11]	Destrucción de información	4	90%	4	4

[email]	Correo electrónico Institucional	[E.1]	Errores de usuarios	5	100%	5	5
		[E.7]	Errores de reencaminamiento	4	90%	4	3
		[E.8]	Errores de secuencia	3	80%	4	3
		[E.11]	Destruccion de información	4	100%	5	5
		[A.3]	Suplantación de identidad	2	60%	2	1
		[A.5]	Uso no previsto	5	100%	5	5
		[A.8]	Repudio	2	50%	2	1
		[A.15]	Denegacion de Servicio	4	100%	5	5
[www]	Internet	[E.2]	Errores de administrador	3	80%	4	3
		[E.7]	Errores de reencaminamiento	3	80%	4	3
		[E.8]	Errores de secuencia	3	80%	4	3
		[E.12]	Fugas de información	4	100%	5	5
		[E.16]	Caida de sistema por agotamiento de recurso	4	100%	5	5
		[A.5]	Uso no previsto	5	100%	5	5
		[A.15]	Denegacion de Servicio	2	60%	5	3
[cont]	Proveedores de T.I	[E.11]	Destruccion de información	2	60%	3	2
		[A.7]	Acceso no autorizado	4	90%	3	2
		[A.11]	Destrucción de información	2	60%	3	2
		[A.12]	Divulgación de información	5	90%	3	3
[s.back]	Servicio de copias de respaldo (bac	[E.2]	Errores de administrador	4	90%	3	3
		[E.12]	Fugas de información	4	90%	4	4
		[A.15]	Denegacion de Servicio	4	100%	4	4
[print]	Servicio de impresión	[E.1]	Errores de usuarios	5	100%	3	3
		[A.15]	Denegacion de Servicio	3	80%	2	2
[sst]	Servicio de Soporte Técnico Interno	[E.10]	Alteración accidental de información	3	80%	4	3
[dns]	Servidor de nombres de dominio	[E.10]	Alteración accidental de información	3	80%	3	3
		[A.7]	Acceso no autorizado	5	90%	3	3
		[A.12]	Divulgación de información	4	90%	4	4
[voip]	Telefonía IP	[E.2]	Errores de administrador	4	90%	3	2
		[E.12]	Fugas de información	3	100%	3	3
		[A.15]	Denegacion de Servicio	3	80%	3	2
SW	**Aplicaciones/Software**						
[browser.1]	Google Chrome	[E.1]	Errores de usuarios	4	80%	4	3
		[E.6]	Disfusión de software dañino	3	60%	5	3
		[E.12]	Fugas de información	4	100%	5	5
		[A.5]	Uso no previsto	5	100%	5	5
[browser.2]	Internet Explorer	[E.1]	Errores de usuarios	5	100%	3	3
		[E.6]	Disfusión de software dañino	3	60%	3	2
		[E.12]	Fugas de información	3	100%	3	3
		[A.5]	Uso no previsto	5	100%	3	3
[av]	Mcafee	[E.1]	Errores de usuarios	5	100%	5	5
		[E.14]	Errores en mantenimiento / Actualizacion de	4	90%	5	5
[office]	Microsof Office	[E.1]	Errores de usuarios	5	100%	3	3
		[E.14]	Errores en mantenimiento / Actualizacion de	4	90%	3	2
		[E.11]	Destruccion de información	2	60%	3	2

[dbms.1]	MySQL	[I.6]	Averías de origen físico o lógico	3	60%	4	2
		[E.1]	Errores de usuarios	5	100%	5	5
		[E.2]	Errores de administrador	4	90%	4	4
		[E.14]	Errores en mantenimiento / Actualizacion de software	4	90%	5	5
		[A.7]	Acceso no autorizado	5	90%	4	4
[dbms.2]	Oracle	[I.6]	Averías de origen físico o lógico	3	60%	4	3
		[E.1]	Errores de usuarios	5	100%	4	4
		[E.2]	Errores de administrador	4	90%	3	3
		[E.14]	Errores en mantenimiento / Actualizacion de software	4	90%	4	4
		[A.7]	Acceso no autorizado	5	90%	3	3
[prp.1]	Sistema Atenciones	[E.1]	Errores de usuarios	5	100%	5	5
		[E.6]	Disfusión de software dañino	3	60%	5	3
		[E.14]	Errores en mantenimiento / Actualizacion de software	4	90%	5	5
		[E.16]	Caida de sistema por agotamiento de recursos.	4	100%	5	5
[a.back]	Sistema de backup	[E.1]	Errores de usuarios	5	100%	5	5
		[E.6]	Disfusión de software dañino	3	60%	5	3
		[E.14]	Errores en mantenimiento / Actualizacion de software	4	90%	5	5
		[E.16]	Caida de sistema por agotamiento de recursos.	4	100%	5	5
[prp.2]	Sistema Myzro	[E.1]	Errores de usuarios	5	100%	5	5
		[E.6]	Disfusión de software dañino	3	60%	5	3
		[E.14]	Errores en mantenimiento / Actualizacion de software	4	90%	5	5
		[E.16]	Caida de sistema por agotamiento de recursos.	4	100%	5	5
[prp.3]	Sistema Ventas	[E.1]	Errores de usuarios	5	100%	4	4
		[E.6]	Disfusión de software dañino	3	60%	4	2
		[E.14]	Errores en mantenimiento / Actualizacion de software	4	90%	4	4
		[E.16]	Caida de sistema por agotamiento de recursos.	4	100%	4	4
[prp.4]	Sistemas General	[E.1]	Errores de usuarios	5	100%	5	5
		[E.6]	Disfusión de software dañino	3	60%	5	3
		[E.14]	Errores en mantenimiento / Actualizacion de software	4	90%	5	4
		[E.16]	Caida de sistema por agotamiento de recursos.	4	100%	5	5
[dbms.3]	SQL Server 2008	[I.6]	Averías de origen físico o lógico	5	100%	4	4
		[E.1]	Errores de usuarios	3	60%	4	2
		[E.2]	Errores de administrador	4	90%	3	3
		[E.14]	Errores en mantenimiento / Actualizacion de software	4	90%	4	3
		[A.7]	Acceso no autorizado	5	90%	3	3
[windows.1]	Windows 7	[E.6]	Disfusión de software dañino	4	75%	5	4
		[E.1]	Errores de usuarios	5	100%	5	5
		[E.11]	Destruccion de información	2	60%	5	3
		[E.12]	Fugas de información	3	90%	5	4
[windows.2]	Windows XP	[E.6]	Disfusión de software dañino	4	75%	3	2
		[E.1]	Errores de usuarios	5	100%	3	3
		[E.11]	Destruccion de información	2	60%	3	2
		[E.12]	Fugas de información	3	90%	3	2

HW	Equipos Informáticos						
[print]	Impresora	[I.4]	Contaminación mecánica	3	60%	4	2
		[I.6]	Averías de origen físico o lógico	5	90%	4	3
		[I.7]	Corte de suministro eléctrico	4	90%	3	3
		[I.8]	Condiciones inadecuadas de temperatura o humedad	3	75%	3	2
		[A.14]	Manipulacion de Equipos	5	90%	4	3
		[A.16]	Robo	5	90%	4	3

[pc.1]	PC Administrativos General	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[I.4]	Contaminación mecánica	3	60%	5	3
		[I.6]	Averías de origen físico o lógico	5	90%	4	4
		[I.7]	Corte de suministro eléctrico	5	90%	3	2
		[E.1]	Errores de usuarios	5	100%	5	5
		[E.4]	Errores de Configuración	4	80%	4	3
		[E.6]	Disfusión de software dañino	5	90%	5	5
		[E.12]	Fugas de información	5	90%	4	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	3	60%	4	2
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	5	5
		[E.17]	Pérdida de equipos	5	90%	5	5
		[A.2]	Manipulación de la configuración	5	100%	5	5
		[A.7]	Acceso no autorizado	5	90%	5	5
		[A.14]	Manipulacion de Equipos	5	90%	4	4
		[A.16]	Robo	4	90%	5	5
[pc.2]	PC Clinica	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[I.4]	Contaminación mecánica	3	60%	5	3
		[I.6]	Averías de origen físico o lógico	5	90%	4	3
		[I.7]	Corte de suministro eléctrico	5	90%	2	2
		[E.1]	Errores de usuarios	5	100%	5	5
		[E.4]	Errores de Configuración	4	80%	4	3
		[E.6]	Disfusión de software dañino	5	90%	5	4
		[E.12]	Fugas de información	5	90%	4	3
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	3	60%	4	2
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	5	5
		[E.17]	Pérdida de equipos	5	90%	5	4
		[A.2]	Manipulación de la configuración	5	100%	5	5
		[A.7]	Acceso no autorizado	4	90%	5	4
		[A.14]	Manipulacion de Equipos	5	90%	4	3
		[A.16]	Robo	5	90%	5	4

[pc.3]	PC Gerencia Administrativa	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[I.4]	Contaminación mecánica	3	60%	5	3
		[I.6]	Averías de origen físico o lógico	5	90%	4	3
		[I.7]	Corte de suministro eléctrico	5	90%	2	2
		[E.1]	Errores de usuarios	5	100%	5	5
		[E.4]	Errores de Configuración	4	80%	4	3
		[E.6]	Disfusión de software dañino	5	90%	5	4
		[E.12]	Fugas de información	4	90%	4	3
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	3	60%	4	2
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	5	5
		[E.17]	Pérdida de equipos	5	90%	5	4
		[A.2]	Manipulación de la configuración	4	100%	5	5
		[A.7]	Acceso no autorizado	5	90%	5	4
		[A.14]	Manipulacion de Equipos	5	90%	4	3
		[A.16]	Robo	5	90%	5	4
[pc.4]	PC Informática	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[I.4]	Contaminación mecánica	3	60%	5	3
		[I.6]	Averías de origen físico o lógico	5	90%	4	4
		[I.7]	Corte de suministro eléctrico	5	90%	3	2
		[E.1]	Errores de usuarios	5	100%	5	5
		[E.4]	Errores de Configuración	4	80%	4	3
		[E.6]	Disfusión de software dañino	5	90%	5	5
		[E.12]	Fugas de información	4	90%	4	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	3	60%	4	2
		[E.16]	Caida de sistema por agotamiento de recursos.	4	100%	5	5
		[E.17]	Pérdida de equipos	5	90%	5	5
		[A.2]	Manipulación de la configuración	5	100%	5	5
		[A.7]	Acceso no autorizado	4	90%	5	5
		[A.14]	Manipulacion de Equipos	5	90%	4	4
		[A.16]	Robo	5	90%	5	5
[pc.5]	PC Jefaturas	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[N.3]	Desastres Naturales	3	60%	5	3
		[I.6]	Averías de origen físico o lógico	5	90%	4	4
		[I.7]	Corte de suministro eléctrico	5	90%	5	5
		[E.1]	Errores de usuarios	5	100%	5	5
		[E.4]	Errores de Configuración	4	80%	4	3
		[E.6]	Disfusión de software dañino	5	90%	5	5
		[E.12]	Fugas de información	5	90%	4	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	3	60%	4	2
		[E.16]	Caida de sistema por agotamiento de recursos.	4	100%	5	5
		[E.17]	Pérdida de equipos	5	90%	5	5
		[A.2]	Manipulación de la configuración	4	100%	5	5
		[A.7]	Acceso no autorizado	4	90%	5	5
		[A.14]	Manipulacion de Equipos	5	90%	4	4
		[A.16]	Robo	4	90%	5	5

[scan]	Scanner	[I.4]	Contaminación mecánica	3	60%	4	2
		[I.6]	Averías de origen físico o lógico	5	90%	4	3
		[I.7]	Corte de suministro eléctrico	4	90%	3	3
		[I.8]	Condiciones inadecuadas de temperatura o humedad	4	70%	3	2
		[A.14]	Manipulacion de Equipos	5	90%	4	3
		[A.16]	Robo	5	90%	4	3
[pabx]	Servidor Central Telefónica	[N.1]	Daños por fuego	2	100%	4	4
		[N.2]	Daños por agua	2	100%	4	4
		[I.4]	Contaminación mecánica	3	60%	4	2
		[I.6]	Averías de origen físico o lógico	5	90%	3	3
		[I.7]	Corte de suministro eléctrico	5	90%	2	2
		[I.8]	Condiciones inadecuadas	2	60%	3	2
		[E.2]	Errores de administrador	5	90%	4	4
		[E.4]	Errores de Configuración	5	90%	3	3
		[E.6]	Disfusión de software dañino	3	60%	4	2
		[E.12]	Fugas de información	4	90%	4	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	5	90%	4	4
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	4	4
		[E.17]	Pérdida de equipos	2	60%	4	2
		[A.4]	Abuso de privilegios de acceso	2	60%	3	2
		[A.5]	Uso no previsto	4	80%	3	3
		[A.7]	Acceso no autorizado	5	90%	2	2
		[A.14]	Manipulacion de Equipos	5	90%	3	3
		[A.15]	Denegacion de Servicio	3	80%	3	3
		[A.16]	Robo	5	90%	4	4
		[A.17]	Ataque destructivo	5	100%	4	4
[servi.1]	Servidor de Backups	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[I.4]	Contaminación mecánica	3	60%	5	3
		[I.6]	Averías de origen físico o lógico	5	90%	5	4
		[I.7]	Corte de suministro eléctrico	5	90%	5	4
		[I.8]	Condiciones inadecuadas	3	60%	5	3
		[E.2]	Errores de administrador	5	90%	4	3
		[E.4]	Errores de Configuración	5	90%	4	3
		[E.6]	Disfusión de software dañino	3	60%	5	3
		[E.12]	Fugas de información	4	90%	5	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	5	90%	5	4
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	5	5
		[E.17]	Pérdida de equipos	2	60%	5	3
		[A.4]	Abuso de privilegios de acceso	2	60%	4	2
		[A.5]	Uso no previsto	3	80%	4	3
		[A.7]	Acceso no autorizado	5	90%	5	4
		[A.14]	Manipulacion de Equipos	5	90%	4	3
		[A.15]	Denegacion de Servicio	4	80%	4	3
		[A.16]	Robo	5	90%	5	4
		[A.17]	Ataque destructivo	5	100%	5	5

[servi.2]	Servidor Myzro	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[I.4]	Contaminación mecánica	1	60%	5	3
		[I.6]	Averías de origen físico o lógico	5	90%	5	5
		[I.7]	Corte de suministro eléctrico	5	90%	5	5
		[I.8]	Condiciones inadecuadas	2	60%	5	3
		[E.2]	Errores de administrador	5	90%	4	4
		[E.4]	Errores de Configuración	5	90%	3	2
		[E.6]	Disfusión de software dañino	3	60%	4	2
		[E.12]	Fugas de información	4	90%	5	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	5	90%	5	5
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	5	5
		[E.17]	Pérdida de equipos	3	60%	5	3
		[A.4]	Abuso de privilegios de acceso	2	60%	4	2
		[A.5]	Uso no previsto	4	80%	4	3
		[A.7]	Acceso no autorizado	5	90%	5	5
		[A.14]	Manipulacion de Equipos	5	90%	4	4
		[A.15]	Denegacion de Servicio	4	80%	4	3
		[A.16]	Robo	5	90%	5	5
		[A.17]	Ataque destructivo	5	100%	5	5
[switch]	Switches	[N.1]	Daños por fuego	2	100%	3	3
		[N.2]	Daños por agua	2	100%	3	3
		[N.3]	Desastres Naturales	2	100%	3	3
		[I.4]	Contaminación mecánica	3	60%	3	2
		[I.6]	Averías de origen físico o lógico	5	90%	3	3
		[I.7]	Corte de suministro eléctrico	5	90%	3	3
		[I.8]	Condiciones inadecuadas	3	60%	3	2
		[E.2]	Errores de administrador	5	90%	2	2
		[E.4]	Errores de Configuración	5	90%	2	2
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	5	90%	2	2
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	3	3
		[E.17]	Pérdida de equipos	3	60%	3	2
		[A.4]	Abuso de privilegios de acceso	2	60%	3	2
		[A.5]	Uso no previsto	5	100%	3	3
		[A.7]	Acceso no autorizado	5	90%	3	3
		[A.14]	Manipulacion de Equipos	5	90%	3	3
		[A.15]	Denegacion de Servicio	5	90%	2	2
		[A.16]	Robo	5	90%	3	3
		[A.17]	Ataque destructivo	5	90%	3	3
SI	**Soportes de Información**						
[san]	Almacenamiento en red	[E.1]	Errores de usuarios	5	100%	5	5
		[E.10]	Alteración accidental de información	5	100%	5	5
		[A.5]	Uso no previsto	4	100%	5	5
		[A.7]	Acceso no autorizado	5	90%	4	4

[cca]	Contratos, convenios, y acuerdos	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[N.3]	Desastres Naturales	2	100%	5	5
		[I.11]	Degradación de los soportes de almacenamiento de la	3	80%	4	3
		[E.10]	Alteración accidental de información	1	60%	3	2
		[E.11]	Destruccion de información	4	100%	5	5
		[E.12]	Fugas de información	4	90%	4	4
		[A.7]	Acceso no autorizado	3	100%	5	5
		[A.10]	Modificación deliberada de información	2	60%	5	3
		[A.11]	Destrucción de información	4	90%	5	5
		[A.12]	Divulgación de información	4	90%	5	5
		[A.16]	Robo	4	90%	5	5
		[A.17]	Ataque destructivo	4	90%	4	4
[printed.1]	Diccionario de Datos	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[N.3]	Desastres Naturales	2	100%	5	5
		[I.4]	Contaminación mecánica	2	60%	3	2
		[I.6]	Averías de origen físico o lógico	2	60%	3	2
		[I.11]	Degradación de los soportes de almacenamiento de la	3	80%	4	3
		[E.10]	Alteración accidental de información	2	60%	3	2
		[E.11]	Destruccion de información	2	60%	5	3
		[E.12]	Fugas de información	4	90%	4	4
		[A.5]	Uso no previsto	3	80%	4	3
		[A.7]	Acceso no autorizado	3	90%	5	5
		[A.10]	Modificación deliberada de información	2	60%	3	2
		[A.11]	Destrucción de información	2	60%	4	2
		[A.12]	Divulgación de información	4	90%	4	4
		[A.16]	Robo	5	90%	5	5
		[A.17]	Ataque destructivo	4	90%	5	5
[disk.2]	Disco Externo	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[N.3]	Desastres Naturales	2	100%	5	5
		[I.4]	Contaminación mecánica	3	60%	4	2
		[I.6]	Averías de origen físico o lógico	3	60%	4	2
		[I.11]	Degradación de los soportes de almacenamiento de la	3	80%	4	3
		[E.10]	Alteración accidental de información	4	80%	4	3
		[E.11]	Destruccion de información	2	100%	5	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	5	90%	4	4
		[E.17]	Pérdida de equipos	4	90%	4	4
		[A.7]	Acceso no autorizado	4	90%	4	4
		[A.10]	Modificación deliberada de información	2	60%	4	2
		[A.11]	Destrucción de información	2	60%	4	2
		[A.14]	Manipulacion de Equipos	4	90%	4	4
		[A.16]	Robo	4	90%	4	4
		[A.17]	Ataque destructivo	4	90%	4	4

[printed.2]	Documentacion de los Sistemas	[N.1]	Daños por fuego	2	100%	4	4
		[N.2]	Daños por agua	2	100%	4	4
		[N.3]	Desastres Naturales	2	100%	4	4
		[I.4]	Contaminación mecánica	2	60%	2	1
		[I.6]	Averías de origen físico o lógico	2	60%	2	1
		[E.2]	Errores de administrador	3	80%	3	3
		[E.10]	Alteración accidental de información	1	60%	2	1
		[E.11]	Destruccion de información	1	60%	4	2
		[E.12]	Fugas de información	4	90%	3	3
		[A.5]	Uso no previsto	3	80%	3	3
		[A.7]	Acceso no autorizado	3	90%	4	4
		[A.10]	Modificación deliberada de información	2	60%	2	1
		[A.11]	Destrucción de información	2	60%	3	2
		[A.12]	Divulgación de información	4	90%	3	3
		[A.16]	Robo	5	90%	5	5
[printed.3]	Informes de Auditoria Médica	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[N.3]	Desastres Naturales	2	100%	5	5
		[I.4]	Contaminación mecánica	2	60%	4	2
		[I.6]	Averías de origen físico o lógico	2	60%	4	2
		[I.11]	Degradación de los soportes de almacenamiento de la	3	80%	4	3
		[E.2]	Errores de administrador	3	80%	4	3
		[E.10]	Alteración accidental de información	1	60%	3	2
		[E.11]	Destruccion de información	1	60%	3	2
		[A.7]	Acceso no autorizado	3	90%	5	5
		[A.10]	Modificación deliberada de información	2	60%	3	2
		[A.11]	Destrucción de información	2	60%	4	2
		[A.12]	Divulgación de información	4	90%	4	4
		[A.16]	Robo	4	90%	5	5
[usb]	USB Administrativos General	[N.1]	Daños por fuego	2	100%	3	3
		[N.2]	Daños por agua	2	100%	3	3
		[N.3]	Desastres Naturales	2	100%	3	3
		[I.4]	Contaminación mecánica	2	60%	2	1
		[I.6]	Averías de origen físico o lógico	2	60%	1	1
		[E.11]	Destruccion de información	1	60%	1	1
		[E.12]	Fugas de información	5	90%	3	3
		[E.17]	Pérdida de equipos	4	90%	3	3
		[A.10]	Modificación deliberada de información	2	60%	2	1
		[A.11]	Destrucción de información	2	60%	2	1
		[A.16]	Robo	4	90%	2	2
AUX	Equipamiento Auxiliar						
[ac]	Aires acondicionados	[N.2]	Daños por agua	2	100%	4	4
		[I.4]	Contaminación mecánica	3	60%	4	2
		[I.6]	Averías de origen físico o lógico	3	60%	4	2
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	5	90%	3	3
[power]	Fuentes de alimentación	[N.2]	Daños por agua	2	100%	4	4
		[I.4]	Contaminación mecánica	3	60%	4	2
		[I.6]	Averías de origen físico o lógico	3	60%	4	2
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	5	90%	3	3

[gen]	Generadores eléctricos	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[I.4]	Contaminación mecánica	3	60%	5	3
		[I.6]	Averías de origen físico o lógico	3	60%	5	3
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	5	90%	4	4
[prp.5]	Sistema de control biometrico dact	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[I.4]	Contaminación mecánica	3	60%	4	2
		[I.6]	Averías de origen físico o lógico	3	60%	4	2
		[I.8]	Condiciones inadecuadas	2	60%	4	2
		[I.10]	Interrupción de otros servicios y suministros esenciale	5	100%	5	5
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	2	60%	4	2
		[E.17]	Pérdida de equipos	4	90%	2	2
		[A.7]	Acceso no autorizado	3	90%	4	3
		[A.16]	Robo	4	90%	5	4
[furniture.1]	Stand Madera Oficinas	[N.1]	Daños por fuego	2	100%	4	4
		[N.2]	Daños por agua	2	100%	4	4
		[N.3]	Desastres Naturales	1	60%	4	2
		[I.6]	Averías de origen físico o lógico	3	60%	3	2
		[I.8]	Condiciones inadecuadas	2	60%	3	2
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	3	80%	3	2
		[E.17]	Pérdida de equipos	4	90%	2	2
		[A.7]	Acceso no autorizado	5	90%	2	2
		[A.16]	Robo	4	90%	4	3
[furniture.2]	Stand Metálica Oficinas	[N.1]	Daños por fuego	2	100%	4	4
		[N.2]	Daños por agua	2	100%	5	5
		[N.3]	Desastres Naturales	1	60%	5	3
		[I.6]	Averías de origen físico o lógico	3	60%	4	2
		[I.8]	Condiciones inadecuadas	3	60%	4	2
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	3	80%	4	3
		[E.17]	Pérdida de equipos	4	90%	3	2
		[A.7]	Acceso no autorizado	5	90%	3	2
		[A.16]	Robo	4	90%	5	5
[ups]	UPS Informática	[N.1]	Daños por fuego	2	100%	4	4
		[N.2]	Daños por agua	2	100%	4	4
		[N.3]	Desastres Naturales	2	100%	4	4
		[I.4]	Contaminación mecánica	3	60%	4	2
		[I.6]	Averías de origen físico o lógico	3	60%	4	2
		[I.8]	Condiciones inadecuadas	2	60%	4	2
		[I.10]	Interrupción de otros servicios y suministros esenciale	5	100%	4	4
		[E.15]	Errores en mantenimiento / Actualizacion de equipos	3	60%	3	2
		[E.17]	Pérdida de equipos	2	60%	4	2
		[A.7]	Acceso no autorizado	4	90%	4	4
		[A.16]	Robo	4	90%	4	4
		[A.17]	Ataque destructivo	4	90%	4	4

COM	Redes de Comunicaciones						
[WAN]	Red de área amplia	[I.9]	Falla de servicios de comunicaciones	4	100%	4	4
		[E.2]	Errores de administrador	4	90%	4	3
		[E.7]	Errores de reencaminamiento	3	100%	4	4
		[E.8]	Errores de secuencia	2	80%	3	2
		[E.10]	Alteración accidental de información	4	80%	3	2
		[E.11]	Destruccion de información	3	60%	4	2
		[E.12]	Fugas de información	5	90%	4	3
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	4	4
		[A.9]	Intercepción de información	3	80%	3	2
		[A.10]	Modificación deliberada de información	4	90%	4	3
		[A.12]	Divulgación de información	4	90%	4	3
		[A.15]	Denegacion de Servicio	5	100%	4	4
[LAN]	Red local	[I.9]	Falla de servicios de comunicaciones	4	100%	4	4
		[E.2]	Errores de administrador	4	90%	4	4
		[E.7]	Errores de reencaminamiento	3	100%	4	4
		[E.8]	Errores de secuencia	2	80%	3	3
		[E.10]	Alteración accidental de información	4	80%	3	3
		[E.11]	Destruccion de información	3	60%	4	2
		[E.12]	Fugas de información	5	90%	4	4
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	4	4
		[A.9]	Intercepción de información	3	80%	3	3
		[A.10]	Modificación deliberada de información	4	90%	4	4
		[A.12]	Divulgación de información	4	90%	4	4
		[A.15]	Denegacion de Servicio	5	100%	4	4
[PSTN]	Red telefónica	[I.9]	Falla de servicios de comunicaciones	4	100%	3	3
		[E.2]	Errores de administrador	4	90%	3	3
		[E.7]	Errores de reencaminamiento	3	100%	3	3
		[E.8]	Errores de secuencia	2	80%	2	2
		[E.10]	Alteración accidental de información	4	80%	2	2
		[E.11]	Destruccion de información	3	60%	3	2
		[E.12]	Fugas de información	5	90%	3	3
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	3	3
		[A.9]	Intercepción de información	3	80%	2	2
		[A.10]	Modificación deliberada de información	4	90%	3	3
		[A.12]	Divulgación de información	4	90%	3	3
		[A.15]	Denegacion de Servicio	5	100%	3	3
[wifi]	Wifi	[I.9]	Falla de servicios de comunicaciones	4	100%	3	3
		[E.2]	Errores de administrador	4	90%	3	3
		[E.7]	Errores de reencaminamiento	3	100%	3	3
		[E.8]	Errores de secuencia	2	80%	3	2
		[E.10]	Alteración accidental de información	4	80%	3	2
		[E.11]	Destruccion de información	3	60%	3	2
		[E.12]	Fugas de información	5	90%	3	3
		[E.16]	Caida de sistema por agotamiento de recursos.	5	100%	3	3
		[A.9]	Intercepción de información	3	80%	3	2
		[A.10]	Modificación deliberada de información	4	90%	3	3
		[A.12]	Divulgación de información	4	90%	3	3
		[A.15]	Denegacion de Servicio	5	100%	3	3

L	Instalaciones						
[building.1]	Edificio Clinica	[N.1]	Daños por fuego	1	60%	4	2
		[N.2]	Daños por agua	2	100%	4	4
		[N.3]	Desastres Naturales	2	100%	4	4
		[E.10]	Alteración accidental de información	4	80%	3	2
		[E.11]	Destruccion de información	4	80%	3	2
		[A.7]	Acceso no autorizado	5	90%	4	3
		[A.17]	Ataque destructivo	5	90%	3	3
		[A.18]	Ocupación enemiga	3	90%	4	3
[building.2]	Edificio Torre Nueva	[N.1]	Daños por fuego	1	60%	3	2
		[N.2]	Daños por agua	2	100%	3	3
		[N.3]	Desastres Naturales	2	100%	3	3
		[E.10]	Alteración accidental de información	4	80%	2	2
		[E.11]	Destruccion de información	4	80%	2	2
		[A.7]	Acceso no autorizado	5	90%	3	3
		[A.17]	Ataque destructivo	5	90%	2	2
		[A.18]	Ocupación enemiga	3	90%	3	3
[local.1]	Oficinas 1 piso	[N.1]	Daños por fuego	2	100%	4	4
		[N.2]	Daños por agua	2	100%	4	4
		[N.3]	Desastres Naturales	2	100%	4	4
		[E.10]	Alteración accidental de información	4	80%	3	3
		[E.11]	Destruccion de información	3	60%	3	2
		[A.7]	Acceso no autorizado	5	90%	4	4
		[A.10]	Modificación deliberada de información	5	90%	3	3
		[A.11]	Destrucción de información	3	60%	3	2
		[A.12]	Divulgación de información	5	90%	2	2
		[A.17]	Ataque destructivo	5	90%	3	3
		[A.18]	Ocupación enemiga	3	90%	4	4
[local.2]	Oficinas 2 piso	[N.1]	Daños por fuego	2	100%	4	4
		[N.2]	Daños por agua	2	100%	4	4
		[N.3]	Desastres Naturales	2	100%	4	4
		[E.10]	Alteración accidental de información	4	80%	3	3
		[E.11]	Destruccion de información	3	60%	3	2
		[A.7]	Acceso no autorizado	5	90%	4	4
		[A.10]	Modificación deliberada de información	5	90%	3	3
		[A.11]	Destrucción de información	3	60%	3	2
		[A.12]	Divulgación de información	5	90%	2	2
		[A.17]	Ataque destructivo	5	90%	3	3
		[A.18]	Ocupación enemiga	3	90%	4	4
[local.3]	Oficinas 3 piso	[N.1]	Daños por fuego	2	100%	4	4
		[N.2]	Daños por agua	2	100%	4	4
		[N.3]	Desastres Naturales	2	100%	4	4
		[E.10]	Alteración accidental de información	4	80%	3	3
		[E.11]	Destruccion de información	3	60%	3	2
		[A.7]	Acceso no autorizado	5	90%	4	4
		[A.10]	Modificación deliberada de información	5	90%	3	3
		[A.11]	Destrucción de información	3	60%	3	2
		[A.12]	Divulgación de información	5	90%	2	2
		[A.17]	Ataque destructivo	5	90%	3	3
		[A.18]	Ocupación enemiga	3	90%	4	4

[local.4]	Sector Consultorios Medicos Clinica	[N.1]	Daños por fuego	2	100%	3	3
		[N.2]	Daños por agua	2	100%	3	3
		[N.3]	Desastres Naturales	2	100%	3	3
		[E.10]	Alteración accidental de información	4	80%	2	2
		[E.11]	Destruccion de información	3	60%	2	1
		[A.7]	Acceso no autorizado	5	90%	3	3
		[A.10]	Modificación deliberada de información	5	90%	2	2
		[A.11]	Destrucción de información	3	60%	2	1
		[A.12]	Divulgación de información	5	90%	2	1
		[A.17]	Ataque destructivo	5	90%	2	2
		[A.18]	Ocupación enemiga	3	90%	3	3
[local.5]	Sector Consultorios Medicos Torre Nueva	[N.1]	Daños por fuego	2	100%	3	3
		[N.2]	Daños por agua	2	100%	3	3
		[N.3]	Desastres Naturales	2	100%	3	3
		[E.10]	Alteración accidental de información	4	80%	3	2
		[E.11]	Destruccion de información	3	60%	3	2
		[A.7]	Acceso no autorizado	5	90%	3	3
		[A.10]	Modificación deliberada de información	5	90%	3	2
		[A.11]	Destrucción de información	3	60%	3	2
		[A.12]	Divulgación de información	5	90%	2	2
		[A.17]	Ataque destructivo	5	90%	3	2
		[A.18]	Ocupación enemiga	3	90%	3	3
[local.6]	Sector Historias Clinicas	[N.1]	Daños por fuego	2	100%	4	4
		[N.2]	Daños por agua	2	100%	4	4
		[N.3]	Desastres Naturales	2	100%	4	4
		[E.10]	Alteración accidental de información	4	80%	3	3
		[E.11]	Destruccion de información	3	60%	3	2
		[A.7]	Acceso no autorizado	5	90%	4	4
		[A.11]	Destrucción de información	3	60%	3	2
		[A.12]	Divulgación de información	5	90%	2	2
		[A.17]	Ataque destructivo	5	90%	3	3
		[A.18]	Ocupación enemiga	3	90%	4	4
[local.7]	Sector Informatica	[N.1]	Daños por fuego	2	100%	5	5
		[N.2]	Daños por agua	2	100%	5	5
		[N.3]	Desastres Naturales	2	100%	5	5
		[E.10]	Alteración accidental de información	5	100%	5	5
		[E.11]	Destruccion de información	3	60%	5	3
		[A.7]	Acceso no autorizado	5	90%	5	5
		[A.10]	Modificación deliberada de información	5	90%	5	5
		[A.11]	Destrucción de información	3	60%	4	2
		[A.12]	Divulgación de información	5	90%	5	5
		[A.17]	Ataque destructivo	5	90%	5	5
		[A.18]	Ocupación enemiga	3	90%	5	5
P	Personal						
[ui.1]	Administrativos General	[E.5]	Deficiencias de la organización	5	90%	3	3
		[E.12]	Fugas de información	4	90%	3	3
		[E.18]	Indisponibilidad del personal	4	90%	3	3
		[A.19]	Indisponibilidad del personal	5	100%	4	4
[ui.2]	Gerencia Administrativa	[E.5]	Deficiencias de la organización	5	90%	4	4
		[E.12]	Fugas de información	4	90%	4	4
		[E.18]	Indisponibilidad del personal	4	90%	4	4
		[A.19]	Indisponibilidad del personal	5	90%	5	5

[ui.3]	Jefaturas	[E.5]	Deficiencias de la organización	5	90%	4	4
		[E.12]	Fugas de información	4	90%	4	4
		[E.18]	Indisponibilidad del personal	4	90%	4	4
		[A.19]	Indisponibilidad del personal	5	100%	5	5
[adm]	Administradores de sistemas	[E.5]	Deficiencias de la organización	5	90%	4	4
		[E.12]	Fugas de información	4	90%	4	4
		[E.18]	Indisponibilidad del personal	4	90%	4	4
		[A.19]	Indisponibilidad del personal	5	100%	5	5
[des]	Desarrolladores/programadores	[E.5]	Deficiencias de la organización	5	90%	4	4
		[E.12]	Fugas de información	4	90%	4	4
		[E.18]	Indisponibilidad del personal	4	90%	4	4
		[A.19]	Indisponibilidad del personal	5	100%	5	5
[ui.4]	Personal Asistencial, Ténicos y Lab	[E.5]	Deficiencias de la organización	5	90%	3	3
		[E.12]	Fugas de información	4	90%	3	3
		[E.18]	Indisponibilidad del personal	4	90%	3	3
		[A.19]	Indisponibilidad del personal	5	100%	4	3
[ui.5]	Personal de Auditoria Medica	[E.5]	Deficiencias de la organización	5	90%	3	3
		[E.12]	Fugas de información	4	90%	3	3
		[E.18]	Indisponibilidad del personal	4	90%	3	3
		[A.19]	Indisponibilidad del personal	5	100%	4	4
[ui.6]	Personal Hist Clinicas	[E.5]	Deficiencias de la organización	5	90%	3	3
		[E.12]	Fugas de información	4	90%	3	3
		[E.18]	Indisponibilidad del personal	4	90%	3	3
		[A.19]	Indisponibilidad del personal	5	100%	4	3

- **Estimación del estado de riesgo potencial y residual**

VALORACION DE ACTIVOS													
Impacto ¿ Cual es la Medida del daño que causa sobre el activo la materialización de una amenaza?													
Probabilidad de Ocurrencia de una amenza sobre un activo : ¿Cuán probable o improbable es que se materialice la amenaza?													
¿Que le podría pasar a los activos si no se protegieran adecuadamente.?													
ACTIVOS POR TIPO		**AMENAZAS**		**POTENCIAL**				**RESIDUAL**					
				IP	**P**	**RP**	**RPT**	**IR**	**PR**	**RR**	**RRT**		
D	**Datos/Información**												
[bd.1]	Base de Datos Atenciones	[E.2]	Errores de administrador	5	5	25		5	5	20			
		[E.4]	Errores de Configuración	4	5	20		3	4	13			
		[E.10]	Alteración accidental de información	4	5	20		2	3	7			
		[E.11]	Destruccion de información	5	5	25	24	5	5	25	18		
		[A.7]	Acceso no autorizado	5	5	25		5	5	20			
		[A.11]	Destrucción de información	5	5	25		5	5	20			
		[A.12]	Divulgación de información	5	5	25		5	5	20			
[bd.2]	Base de Datos General	[E.2]	Errores de administrador	4	5	22		4	5	18			
		[E.4]	Errores de Configuración	3	5	17		3	4	11			
		[E.10]	Alteración accidental de información	3	5	17		2	3	6			
		[E.11]	Destruccion de información	4	5	22	20	4	5	22	16		
		[A.7]	Acceso no autorizado	4	5	22		4	5	18			
		[A.11]	Destrucción de información	4	5	22		4	5	18			
		[A.12]	Divulgación de información	4	5	22		4	5	18			
[bd.3]	Base de Datos Myzro	[E.2]	Errores de administrador	4	5	19		3	5	15			
		[E.4]	Errores de Configuración	4	5	19		3	4	12			
		[E.10]	Alteración accidental de información	4	5	19		2	3	7			
		[E.11]	Destruccion de información	5	5	23	21	5	5	23	16		
		[A.7]	Acceso no autorizado	5	5	23		4	5	19			
		[A.11]	Destrucción de información	5	5	23		4	5	19			
		[A.12]	Divulgación de información	5	5	23		4	5	19			
[bd.4]	Base de Datos Ventas	[E.2]	Errores de administrador	5	5	25		5	5	20			
		[E.4]	Errores de Configuración	4	5	20		3	4	13			
		[E.10]	Alteración accidental de información	4	4	16		2	2	6			
		[E.11]	Destruccion de información	5	3	15	20	5	3	15	15		
		[A.7]	Acceso no autorizado	5	4	20		5	4	16			
		[A.11]	Destrucción de información	5	5	25		5	5	20			
		[A.12]	Divulgación de información	5	4	20		5	4	16			
[exe]	Codigo ejecutable	[E.2]	Errores de administrador	3	5	17		3	5	14			
		[E.3]	Errores de Monitorización	4	5	22	20	4	5	22	19		
		[E.11]	Destruccion de información	4	5	22		4	5	22			
[source.1]	Codigo Fuente Atenciones	[E.2]	Errores de administrador	4	5	22		4	5	18			
		[E.4]	Errores de Configuración	3	5	17		3	4	11			
		[E.10]	Alteración accidental de información	3	4	14		2	2	5			
		[E.11]	Destruccion de información	4	4	17	19	4	4	17	13		
		[A.7]	Acceso no autorizado	4	5	22		3	4	12			
		[A.11]	Destrucción de información	4	5	22		3	3	8			
		[A.12]	Divulgación de información	4	5	22		4	5	18			
[source.2]	Codigo Fuente Myzro	[E.2]	Errores de administrador	5	5	23		4	5	19			
		[E.4]	Errores de Configuración	4	5	19		3	4	12			
		[E.10]	Alteración accidental de información	4	5	19		2	3	7			
		[E.11]	Destruccion de información	5	4	19	21	5	4	19	13		
		[A.7]	Acceso no autorizado	5	4	19		4	3	11			
		[A.11]	Destrucción de información	5	5	23		3	3	8			
		[A.12]	Divulgación de información	5	5	23		4	5	19			

[source.3]	Codigo Fuente Ventas	[E.2]	Errores de administrador	4	4	17	17	4	4	14	13		
		[E.4]	Errores de Configuración	4	5	22		4	5	22			
		[E.10]	Alteración accidental de información	3	4	14		2	2	5			
		[E.11]	Destruccion de información	4	4	17		4	4	17			
		[A.7]	Acceso no autorizado	3	5	17		3	4	10			
		[A.11]	Destrucción de información	4	4	17		3	2	6			
		[A.12]	Divulgación de información	4	4	17		4	4	14			
[backup]	Copias de respaldo	[E.11]	Destruccion de información	5	5	23	19	5	5	23	18		
		[E.12]	Fugas de información	4	4	15		3	4	12			
		[A.11]	Destrucción de información	5	4	19		5	4	19			
[password]	Credenciales (contraseñas)	[E.11]	Destruccion de información	4	5	18	15	2	3	7	10		
		[E.12]	Fugas de información	3	4	12		3	4	10			
		[A.11]	Destrucción de información	4	4	15		4	4	15			
[conf]	Datos de configuración	[E.4]	Errores de Configuración	3	5	13	15	2	4	9	15		
		[E.11]	Destruccion de información	3	5	17		3	5	14			
		[E.12]	Fugas de información	3	5	13		2	4	9			
		[A.11]	Destrucción de información	3	5	17		3	5	17			
[email]	Correo electrónico Institucional	[E.1]	Errores de usuarios	5	5	23	16	5	5	23	14		
		[E.7]	Errores de reencaminamiento	4	4	15		3	4	12			
		[E.8]	Errores de secuencia	4	4	15		3	3	10			
		[E.11]	Destruccion de información	5	4	19		5	4	19			
		[A.3]	Suplantación de identidad	2	4	9		1	2	3			
		[A.5]	Uso no previsto	5	5	23		5	5	23			
		[A.8]	Repudio	2	3	7		1	2	2			
		[A.15]	Denegacion de Servicio	5	4	19		5	4	19			
[www]	Internet	[E.2]	Errores de administrador	4	4	16	19	3	3	10	15		
		[E.7]	Errores de reencaminamiento	4	4	16		3	3	10			
		[E.8]	Errores de secuencia	4	4	16		3	3	10			
		[E.12]	Fugas de información	5	4	20		5	4	20			
		[E.16]	Caida de sistema por agotamiento de recurso	5	4	20		5	4	20			
		[A.5]	Uso no previsto	5	5	25		5	5	25			
		[A.15]	Denegacion de Servicio	5	4	20		3	2	7			
[cont]	Proveedores de T.I	[E.11]	Destruccion de información	3	4	13	14	2	2	5	8		
		[A.7]	Acceso no autorizado	3	4	11		2	4	9			
		[A.11]	Destrucción de información	3	4	13		2	2	5			
		[A.12]	Divulgación de información	3	5	17		3	5	14			
[acl]	Datos de control de acceso	[E.11]	Destruccion de información	5	5	25	20	5	5	20	13		
		[E.12]	Fugas de información	4	4	16		3	3	10			
		[A.11]	Destrucción de información	5	4	20		3	2	7			
[test]	Datos de prueba	[E.11]	Destruccion de información	3	5	15	12	3	5	12	9		
		[E.12]	Fugas de información	2	4	10		2	3	6			
		[A.11]	Destrucción de información	3	4	12		3	4	10			
[files]	Ficheros	[E.11]	Destruccion de información	4	5	20	15	4	5	16	12		
		[E.12]	Fugas de información	3	4	13		3	3	8			
		[A.1]	Manipulación de los registros de actividad (lo	4	3	12		4	3	12			
		[A.11]	Destrucción de información	4	4	16		4	4	13			
[hc]	Historias Clinicas	[E.11]	Destruccion de información	5	5	23	18	4	5	19	14		
		[E.12]	Fugas de información	4	4	15		3	3	10			
		[A.7]	Acceso no autorizado	4	3	11		3	3	9			
		[A.11]	Destrucción de información	5	5	23		4	5	19			
S	**Servicios**												
[file]	Almacenamiento de ficheros	[E.11]	Destruccion de información	5	4	20	19	4	3	11	14		
		[E.12]	Fugas de información	5	4	20		5	4	16			
		[A.7]	Acceso no autorizado	4	5	20		4	5	16			
		[A.11]	Destrucción de información	4	4	16		4	4	13			

[email]	Correo electrónico Institucional	[E.1]	Errores de usuarios	5	5	23	16	5	5	23	14
		[E.7]	Errores de reencaminamiento	4	4	15		3	4	12	
		[E.8]	Errores de secuencia	4	4	15		3	3	10	
		[E.11]	Destruccion de información	5	4	19		5	4	19	
		[A.3]	Suplantación de identidad	2	4	9		1	2	3	
		[A.5]	Uso no previsto	5	5	23		5	5	23	
		[A.8]	Repudio	2	3	7		1	2	2	
		[A.15]	Denegacion de Servicio	5	4	19		5	4	19	
[www]	Internet	[E.2]	Errores de administrador	4	4	16	19	3	3	10	15
		[E.7]	Errores de reencaminamiento	4	4	16		3	3	10	
		[E.8]	Errores de secuencia	4	4	16		3	3	10	
		[E.12]	Fugas de información	5	4	20		5	4	20	
		[E.16]	Caida de sistema por agotamiento de recurso	5	4	20		5	4	20	
		[A.5]	Uso no previsto	5	5	25		5	5	25	
		[A.15]	Denegacion de Servicio	5	4	20		3	2	7	
[cont]	Proveedores de T.I	[E.11]	Destruccion de información	3	4	13	14	2	2	5	8
		[A.7]	Acceso no autorizado	3	4	11		2	4	9	
		[A.11]	Destrucción de información	3	4	13		2	2	5	
		[A.12]	Divulgación de información	3	5	17		3	5	14	
[s.back]	Servicio de copias de respaldo (backu	[E.2]	Errores de administrador	3	4	13	15	3	4	10	13
		[E.12]	Fugas de información	4	4	16		4	4	13	
		[A.15]	Denegacion de Servicio	4	4	16		4	4	16	
[print]	Servicio de impresión	[E.1]	Errores de usuarios	3	5	15	12	3	5	15	11
		[A.15]	Denegacion de Servicio	2	4	10		2	3	6	
[sst]	Servicio de Soporte Técnico Interno	[E.10]	Alteración accidental de información	4	4	15	15	3	3	10	10
[dns]	Servidor de nombres de dominio	[E.10]	Alteración accidental de información	3	4	13	15	3	3	8	11
		[A.7]	Acceso no autorizado	3	5	16		3	5	13	
		[A.12]	Divulgación de información	4	4	16		4	4	13	
[voip]	Telefonía IP	[E.2]	Errores de administrador	3	4	11	10	2	4	9	8
		[E.12]	Fugas de información	3	3	10		3	3	10	
		[A.15]	Denegacion de Servicio	3	4	11		2	3	7	
SW	**Aplicaciones/Software**										
[browser.1]	Google Chrome	[E.1]	Errores de usuarios	4	5	19	21	3	4	12	16
		[E.6]	Disfusión de software dañino	5	5	23		3	3	8	
		[E.12]	Fugas de información	5	4	19		5	4	19	
		[A.5]	Uso no previsto	5	5	23		5	5	23	
[browser.2]	Internet Explorer	[E.1]	Errores de usuarios	3	5	13	12	3	5	13	10
		[E.6]	Disfusión de software dañino	3	5	13		2	3	5	
		[E.12]	Fugas de información	3	3	8		3	3	8	
		[A.5]	Uso no previsto	3	5	13		3	5	13	
[av]	Mcafee	[E.1]	Errores de usuarios	5	5	25	23	5	5	25	21
		[E.14]	Errores en mantenimiento / Actualizacion de	5	4	20		5	4	16	
[office]	Microsof Office	[E.1]	Errores de usuarios	3	5	13	12	3	5	13	9
		[E.14]	Errores en mantenimiento / Actualizacion de	3	4	11		2	4	9	
		[E.11]	Destruccion de información	3	4	11		2	2	4	
[dbms.1]	MySQL	[I.6]	Averías de origen físico o lógico	4	5	20	20	2	3	7	16
		[E.1]	Errores de usuarios	5	5	25		5	5	25	
		[E.2]	Errores de administrador	4	4	16		4	4	13	
		[E.14]	Errores en mantenimiento / Actualizacion de	5	4	20		5	4	16	
		[A.7]	Acceso no autorizado	4	5	20		4	5	16	
[dbms.2]	Oracle	[I.6]	Averías de origen físico o lógico	4	5	22	18	3	3	8	14
		[E.1]	Errores de usuarios	4	5	22		4	5	22	
		[E.2]	Errores de administrador	3	4	14		3	4	11	
		[E.14]	Errores en mantenimiento / Actualizacion de	4	4	17		4	4	14	
		[A.7]	Acceso no autorizado	3	5	17		3	5	14	

[pc.1]	PC Administrativos General	[N.1]	Daños por fuego	5	2	10	20	5	2	10	16
		[N.2]	Daños por agua	5	2	10		5	2	10	
		[I.4]	Contaminación mecánica	5	5	25		3	3	9	
		[I.6]	Averías de origen físico o lógico	4	5	20		4	5	16	
		[I.7]	Corte de suministro eléctrico	3	5	13		2	5	10	
		[E.1]	Errores de usuarios	5	5	25		5	5	25	
		[E.4]	Errores de Configuración	4	5	20		3	4	13	
		[E.6]	Disfusión de software dañino	5	5	25		5	5	20	
		[E.12]	Fugas de información	4	5	20		4	5	16	
		[E.15]	Errores en mantenimiento / Actualizacion de	4	5	20		2	3	7	
		[E.16]	Caida de sistema por agotamiento de recurso	5	5	25		5	5	25	
		[E.17]	Pérdida de equipos	5	5	25		5	5	20	
		[A.2]	Manipulación de la configuración	5	5	25		5	5	25	
		[A.7]	Acceso no autorizado	5	5	25		5	5	20	
		[A.14]	Manipulacion de Equipos	4	5	20		4	5	16	
		[A.16]	Robo	5	4	20		5	4	16	
[prp.3]	Sistema Ventas	[E.1]	Errores de usuarios	4	5	20	18	4	5	20	14
		[E.6]	Disfusión de software dañino	4	5	20		2	3	7	
		[E.14]	Errores en mantenimiento / Actualizacion de	4	4	16		4	4	13	
		[E.16]	Caida de sistema por agotamiento de recurso	4	4	16		4	4	16	
[prp.4]	Sistemas General	[E.1]	Errores de usuarios	5	5	23	21	5	5	23	16
		[E.6]	Disfusión de software dañino	5	5	23		3	3	8	
		[E.14]	Errores en mantenimiento / Actualizacion de	5	4	19		4	4	15	
		[E.16]	Caida de sistema por agotamiento de recurso	5	4	19		5	4	19	
[dbms.3]	SQL Server 2008	[I.6]	Averías de origen físico o lógico	4	5	18	16	4	5	18	12
		[E.1]	Errores de usuarios	4	5	18		2	3	7	
		[E.2]	Errores de administrador	3	4	12		3	4	10	
		[E.14]	Errores en mantenimiento / Actualizacion de	4	4	15		3	4	12	
		[A.7]	Acceso no autorizado	3	5	15		3	5	12	
[windows.1]	Windows 7	[E.6]	Disfusión de software dañino	5	5	23	20	4	4	13	14
		[E.1]	Errores de usuarios	5	5	23		5	5	23	
		[E.11]	Destruccion de información	5	4	19		3	2	7	
		[E.12]	Fugas de información	5	3	14		4	3	11	
[windows.2]	Windows XP	[E.6]	Disfusión de software dañino	3	5	13	11	2	4	8	8
		[E.1]	Errores de usuarios	3	5	13		3	5	13	
		[E.11]	Destruccion de información	3	4	11		2	2	4	
		[E.12]	Fugas de información	3	3	8		2	3	6	
HW	**Equipos Informáticos**										
[print]	Impresora	[I.4]	Contaminación mecánica	4	5	18	16	2	3	7	11
		[I.6]	Averías de origen físico o lógico	4	5	18		3	5	15	
		[I.7]	Corte de suministro eléctrico	3	4	12		3	4	10	
		[I.8]	Condiciones inadecuadas de temperatura o h	3	4	12		2	3	7	
		[A.14]	Manipulacion de Equipos	4	5	18		3	5	15	
		[A.16]	Robo	4	5	18		3	5	15	

[pc.2]	PC Clinica	[N.1]	Daños por fuego	5	2	9	19	5	2	9	15
		[N.2]	Daños por agua	5	2	9		5	2	9	
		[I.4]	Contaminación mecánica	5	5	23		3	3	8	
		[I.6]	Averías de origen físico o lógico	4	5	19		3	5	15	
		[I.7]	Corte de suministro eléctrico	2	5	12		2	5	9	
		[E.1]	Errores de usuarios	5	5	23		5	5	23	
		[E.4]	Errores de Configuración	4	5	19		3	4	12	
		[E.6]	Disfusión de software dañino	5	5	23		4	5	19	
		[E.12]	Fugas de información	4	5	19		3	5	15	
		[E.15]	Errores en mantenimiento / Actualizacion de	4	5	19		2	3	7	
		[E.16]	Caida de sistema por agotamiento de recurso	5	5	23		5	5	23	
		[E.17]	Pérdida de equipos	5	5	23		4	5	19	
		[A.2]	Manipulación de la configuración	5	5	23		5	5	23	
		[A.7]	Acceso no autorizado	5	4	19		4	4	15	
		[A.14]	Manipulacion de Equipos	4	5	19		3	5	15	
		[A.16]	Robo	5	5	23		4	5	19	
[pc.3]	PC Gerencia Administrativa	[N.1]	Daños por fuego	5	2	9	19	5	2	9	15
		[N.2]	Daños por agua	5	2	9		5	2	9	
		[I.4]	Contaminación mecánica	5	5	23		3	3	8	
		[I.6]	Averías de origen físico o lógico	4	5	19		3	5	15	
		[I.7]	Corte de suministro eléctrico	2	5	12		2	5	9	
		[E.1]	Errores de usuarios	5	5	23		5	5	23	
		[E.4]	Errores de Configuración	4	5	19		3	4	12	
		[E.6]	Disfusión de software dañino	5	5	23		4	5	19	
		[E.12]	Fugas de información	4	4	15		3	4	12	
		[E.15]	Errores en mantenimiento / Actualizacion de	4	5	19		2	3	7	
		[E.16]	Caida de sistema por agotamiento de recurso	5	5	23		5	5	23	
		[E.17]	Pérdida de equipos	5	5	23		4	5	19	
		[A.2]	Manipulación de la configuración	5	4	19		5	4	19	
		[A.7]	Acceso no autorizado	5	5	23		4	5	19	
		[A.14]	Manipulacion de Equipos	4	5	19		3	5	15	
		[A.16]	Robo	5	5	23		4	5	19	
[pc.4]	PC Informática	[N.1]	Daños por fuego	5	2	10	20	5	2	10	16
		[N.2]	Daños por agua	5	2	10		5	2	10	
		[I.4]	Contaminación mecánica	5	5	25		3	3	9	
		[I.6]	Averías de origen físico o lógico	4	5	20		4	5	16	
		[I.7]	Corte de suministro eléctrico	3	5	13		2	5	10	
		[E.1]	Errores de usuarios	5	5	25		5	5	25	
		[E.4]	Errores de Configuración	4	5	20		3	4	13	
		[E.6]	Disfusión de software dañino	5	5	25		5	5	20	
		[E.12]	Fugas de información	4	4	16		4	4	13	
		[E.15]	Errores en mantenimiento / Actualizacion de	4	5	20		2	3	7	
		[E.16]	Caida de sistema por agotamiento de recurso	5	4	20		5	4	20	
		[E.17]	Pérdida de equipos	5	5	25		5	5	20	
		[A.2]	Manipulación de la configuración	5	5	25		5	5	25	
		[A.7]	Acceso no autorizado	5	4	20		5	4	16	
		[A.14]	Manipulacion de Equipos	4	5	20		4	5	16	
		[A.16]	Robo	5	5	25		5	5	20	

[pc.5]	PC Jefaturas	[N.1]	Daños por fuego	5	2	10	20	5	2	10	16
		[N.2]	Daños por agua	5	2	10		5	2	10	
		[N.3]	Desastres Naturales	5	5	25		3	3	9	
		[I.6]	Averías de origen físico o lógico	4	5	20		4	5	16	
		[I.7]	Corte de suministro eléctrico	5	5	25		5	5	20	
		[E.1]	Errores de usuarios	5	5	25		5	5	25	
		[E.4]	Errores de Configuración	4	5	20		3	4	13	
		[E.6]	Disfusión de software dañino	5	5	25		5	5	20	
		[E.12]	Fugas de información	4	5	20		4	5	16	
		[E.15]	Errores en mantenimiento / Actualizacion de	4	5	20		2	3	7	
		[E.16]	Caida de sistema por agotamiento de recurso	5	4	20		5	4	20	
		[E.17]	Pérdida de equipos	5	5	25		5	5	20	
		[A.2]	Manipulación de la configuración	5	4	20		5	4	20	
		[A.7]	Acceso no autorizado	5	4	20		5	4	16	
		[A.14]	Manipulacion de Equipos	4	5	20		4	5	16	
		[A.16]	Robo	5	4	20		5	4	16	
[scan]	Scanner	[I.4]	Contaminación mecánica	4	5	18	17	2	3	7	11
		[I.6]	Averías de origen físico o lógico	4	5	18		3	5	15	
		[I.7]	Corte de suministro eléctrico	3	4	12		3	4	10	
		[I.8]	Condiciones inadecuadas de temperatura o h	3	5	15		2	4	7	
		[A.14]	Manipulacion de Equipos	4	5	18		3	5	15	
		[A.16]	Robo	4	5	18		3	5	15	
[pabx]	Servidor Central Telefónica	[N.1]	Daños por fuego	4	2	8	16	4	2	8	11
		[N.2]	Daños por agua	4	2	8		4	2	8	
		[I.4]	Contaminación mecánica	4	5	20		2	3	7	
		[I.6]	Averías de origen físico o lógico	3	5	16		3	5	13	
		[I.7]	Corte de suministro eléctrico	2	5	10		2	5	8	
		[I.8]	Condiciones inadecuadas	3	4	13		2	2	5	
		[E.2]	Errores de administrador	4	5	20		4	5	16	
		[E.4]	Errores de Configuración	3	5	16		3	5	13	
		[E.6]	Disfusión de software dañino	4	5	20		2	3	7	
		[E.12]	Fugas de información	4	4	16		4	4	13	
		[E.15]	Errores en mantenimiento / Actualizacion de	4	5	20		4	5	16	
		[E.16]	Caida de sistema por agotamiento de recurso	4	5	20		4	5	20	
		[E.17]	Pérdida de equipos	4	4	16		2	2	6	
		[A.4]	Abuso de privilegios de acceso	3	4	13		2	2	5	
		[A.5]	Uso no previsto	3	5	16		3	4	10	
		[A.7]	Acceso no autorizado	2	5	10		2	5	8	
		[A.14]	Manipulacion de Equipos	3	5	16		3	5	13	
		[A.15]	Denegacion de Servicio	3	4	13		3	3	8	
		[A.16]	Robo	4	5	20		4	5	16	

		[A.17]	Ataque destructivo	4	5	20		4	5	20			
[servi.1]	Servidor de Backups	[N.1]	Daños por fuego	5	2	9		5	2	9			
		[N.2]	Daños por agua	5	2	9		5	2	9			
		[I.4]	Contaminación mecánica	5	5	23		3	3	8			
		[I.6]	Averías de origen físico o lógico	5	5	23		4	5	19			
		[I.7]	Corte de suministro eléctrico	5	5	23		4	5	19			
		[I.8]	Condiciones inadecuadas	5	5	23		3	3	8			
		[E.2]	Errores de administrador	4	5	19		3	5	15			
		[E.4]	Errores de Configuración	4	5	19		3	5	15			
		[E.6]	Disfusión de software dañino	5	5	23		3	3	8			
		[E.12]	Fugas de información	5	4	19		4	4	15			
		[E.15]	Errores en mantenimiento / Actualizacion de	5	5	23	20	4	5	19	14		
		[E.16]	Caida de sistema por agotamiento de recurso	5	5	23		5	5	23			
		[E.17]	Pérdida de equipos	5	4	19		3	2	7			
		[A.4]	Abuso de privilegios de acceso	4	3	11		2	2	4			
		[A.5]	Uso no previsto	4	4	15		3	3	10			
		[A.7]	Acceso no autorizado	5	5	23		4	5	19			
		[A.14]	Manipulacion de Equipos	4	5	19		3	5	15			
		[A.15]	Denegacion de Servicio	4	5	19		3	4	12			
		[A.16]	Robo	5	5	23		4	5	19			
		[A.17]	Ataque destructivo	5	5	23		5	5	23			
[servi.2]	Servidor Myzro	[N.1]	Daños por fuego	5	2	10		5	2	10			
		[N.2]	Daños por agua	5	2	10		5	2	10			
		[I.4]	Contaminación mecánica	5	2	10		3	1	4			
		[I.6]	Averías de origen físico o lógico	5	5	25		5	5	20			
		[I.7]	Corte de suministro eléctrico	5	5	25		5	5	20			
		[I.8]	Condiciones inadecuadas	5	4	20		3	2	7			
		[E.2]	Errores de administrador	4	5	20		4	5	16			
		[E.4]	Errores de Configuración	3	5	13		2	5	10			
		[E.6]	Disfusión de software dañino	4	5	20		2	3	7			
		[E.12]	Fugas de información	5	4	20		5	4	16			
		[E.15]	Errores en mantenimiento / Actualizacion de	5	5	25	20	5	5	20	14		
		[E.16]	Caida de sistema por agotamiento de recurso	5	5	25		5	5	25			
		[E.17]	Pérdida de equipos	5	5	25		3	3	9			
		[A.4]	Abuso de privilegios de acceso	4	4	16		2	2	6			
		[A.5]	Uso no previsto	4	5	20		3	4	13			
		[A.7]	Acceso no autorizado	5	5	25		5	5	20			
		[A.14]	Manipulacion de Equipos	4	5	20		4	5	16			
		[A.15]	Denegacion de Servicio	4	5	20		3	4	13			
		[A.16]	Robo	5	5	25		5	5	20			
		[A.17]	Ataque destructivo	5	5	25		5	5	25			
[switch]	Switches	[N.1]	Daños por fuego	3	2	6		3	2	6			
		[N.2]	Daños por agua	3	2	6		3	2	6			
		[N.3]	Desastres Naturales	3	2	6		3	2	6			
		[I.4]	Contaminación mecánica	3	5	15		2	3	5			
		[I.6]	Averías de origen físico o lógico	3	5	15		3	5	12			
		[I.7]	Corte de suministro eléctrico	3	5	15		3	5	12			
		[I.8]	Condiciones inadecuadas	3	5	15		2	3	5			
		[E.2]	Errores de administrador	2	5	12		2	5	10			
		[E.4]	Errores de Configuración	2	5	12		2	5	10			
		[E.15]	Errores en mantenimiento / Actualizacion de	2	5	12	13	2	5	10	9		
		[E.16]	Caida de sistema por agotamiento de recurso	3	5	15		3	5	15			
		[E.17]	Pérdida de equipos	3	5	15		2	3	5			
		[A.4]	Abuso de privilegios de acceso	3	4	12		2	2	4			
		[A.5]	Uso no previsto	3	5	15		3	5	15			
		[A.7]	Acceso no autorizado	3	5	15		3	5	12			
		[A.14]	Manipulacion de Equipos	3	5	15		3	5	12			

		[A.15]	Denegacion de Servicio	2	5	12		2	5	10			
		[A.16]	Robo	3	5	15		3	5	12			
		[A.17]	Ataque destructivo	3	5	15		3	5	12			
SI	**Soportes de Información**												
[san]	Almacenamiento en red	[E.1]	Errores de usuarios	5	5	25		5	5	25			
		[E.10]	Alteración accidental de información	5	5	25	23	5	5	25	22		
		[A.5]	Uso no previsto	5	4	20		5	4	20			
		[A.7]	Acceso no autorizado	4	5	20		4	5	16			
[cca]	Contratos, convenios, y acuerdos	[N.1]	Daños por fuego	5	2	10		5	2	10			
		[N.2]	Daños por agua	5	2	10		5	2	10			
		[N.3]	Desastres Naturales	5	2	10		5	2	10			
		[I.11]	Degradación de los soportes de almacenamie	4	4	16		3	3	10			
		[E.10]	Alteración accidental de información	3	2	5		2	1	2			
		[E.11]	Destruccion de información	5	4	20		5	4	20			
		[E.12]	Fugas de información	4	4	16	15	4	4	13	12		
		[A.7]	Acceso no autorizado	5	3	15		5	3	15			
		[A.10]	Modificación deliberada de información	5	3	15		3	2	5			
		[A.11]	Destrucción de información	5	4	20		5	4	16			
		[A.12]	Divulgación de información	5	4	20		5	4	16			
		[A.16]	Robo	5	4	20		5	4	16			
		[A.17]	Ataque destructivo	4	4	16		4	4	13			
[printed.1]	Diccionario de Datos	[N.1]	Daños por fuego	5	2	10		5	2	10			
		[N.2]	Daños por agua	5	2	10		5	2	10			
		[N.3]	Desastres Naturales	5	2	10		5	2	10			
		[I.4]	Contaminación mecánica	3	4	10		2	2	4			
		[I.6]	Averías de origen físico o lógico	3	4	10		2	2	4			
		[I.11]	Degradación de los soportes de almacenamie	4	4	16		3	3	10			
		[E.10]	Alteración accidental de información	3	4	10		2	2	4			
		[E.11]	Destruccion de información	5	4	20	14	3	2	7	9		
		[E.12]	Fugas de información	4	4	16		4	4	13			
		[A.5]	Uso no previsto	4	4	16		3	3	10			
		[A.7]	Acceso no autorizado	5	3	15		5	3	12			
		[A.10]	Modificación deliberada de información	3	3	8		2	2	3			
		[A.11]	Destrucción de información	4	4	16		2	2	6			
		[A.12]	Divulgación de información	4	4	16		4	4	13			
		[A.16]	Robo	5	5	25		5	5	20			
		[A.17]	Ataque destructivo	5	4	20		5	4	16			
[disk.2]	Disco Externo	[N.1]	Daños por fuego	5	2	10		5	2	10			
		[N.2]	Daños por agua	5	2	10		5	2	10			
		[N.3]	Desastres Naturales	5	2	10		5	2	10			
		[I.4]	Contaminación mecánica	4	5	20		2	3	7			
		[I.6]	Averías de origen físico o lógico	4	5	20		2	3	7			
		[I.11]	Degradación de los soportes de almacenamie	4	4	16		3	3	10			
		[E.10]	Alteración accidental de información	4	5	20		3	4	13			
		[E.11]	Destruccion de información	5	2	10	15	5	2	10	10		
		[E.15]	Errores en mantenimiento / Actualizacion de	4	5	20		4	5	16			
		[E.17]	Pérdida de equipos	4	4	16		4	4	13			
		[A.7]	Acceso no autorizado	4	4	16		4	4	13			
		[A.10]	Modificación deliberada de información	4	3	12		2	2	4			
		[A.11]	Destrucción de información	4	3	12		2	2	4			
		[A.14]	Manipulacion de Equipos	4	4	16		4	4	13			
		[A.16]	Robo	4	4	16		4	4	13			
		[A.17]	Ataque destructivo	4	4	16		4	4	13			

[printed.2]	Documentacion de los Sistemas	[N.1]	Daños por fuego	4	2	8	11	4	2	8	7		
		[N.2]	Daños por agua	4	2	8		4	2	8			
		[N.3]	Desastres Naturales	4	2	8		4	2	8			
		[I.4]	Contaminación mecánica	2	4	8		1	2	3			
		[I.6]	Averías de origen físico o lógico	2	4	8		1	2	3			
		[E.2]	Errores de administrador	3	4	13		3	3	8			
		[E.10]	Alteración accidental de información	2	2	4		1	1	1			
		[E.11]	Destruccion de información	4	2	8		2	1	3			
		[E.12]	Fugas de información	3	4	13		3	4	10			
		[A.5]	Uso no previsto	3	4	13		3	3	8			
		[A.7]	Acceso no autorizado	4	3	12		4	3	10			
		[A.10]	Modificación deliberada de información	2	3	6		1	2	2			
		[A.11]	Destrucción de información	3	4	13		2	2	5			
		[A.12]	Divulgación de información	3	4	13		3	4	10			
		[A.16]	Robo	5	5	25		5	5	20			
[printed.3]	Informes de Auditoria Médica	[N.1]	Daños por fuego	5	2	10	14	5	2	10	9		
		[N.2]	Daños por agua	5	2	10		5	2	10			
		[N.3]	Desastres Naturales	5	2	10		5	2	10			
		[I.4]	Contaminación mecánica	4	4	16		2	2	6			
		[I.6]	Averías de origen físico o lógico	4	4	16		2	2	6			
		[I.11]	Degradación de los soportes de almacenamie	4	4	16		3	3	10			
		[E.2]	Errores de administrador	4	4	16		3	3	10			
		[E.10]	Alteración accidental de información	3	2	5		2	1	2			
		[E.11]	Destruccion de información	3	2	5		2	1	2			
		[A.7]	Acceso no autorizado	5	3	15		5	3	12			
		[A.10]	Modificación deliberada de información	3	3	8		2	2	3			
		[A.11]	Destrucción de información	4	4	16		2	2	6			
		[A.12]	Divulgación de información	4	4	16		4	4	13			
		[A.16]	Robo	5	4	20		5	4	16			
[usb]	USB Administrativos General	[N.1]	Daños por fuego	3	2	6	8	3	2	6	5		
		[N.2]	Daños por agua	3	2	6		3	2	6			
		[N.3]	Desastres Naturales	3	2	6		3	2	6			
		[I.4]	Contaminación mecánica	2	3	5		1	2	2			
		[I.6]	Averías de origen físico o lógico	1	3	3		1	2	1			
		[E.11]	Destruccion de información	1	2	2		1	1	1			
		[E.12]	Fugas de información	3	5	15		3	5	12			
		[E.17]	Pérdida de equipos	3	4	12		3	4	10			
		[A.10]	Modificación deliberada de información	2	4	10		1	2	3			
		[A.11]	Destrucción de información	2	4	10		1	2	3			
		[A.16]	Robo	2	4	10		2	4	8			
AUX	**Equipamiento Auxiliar**												
[ac]	Aires acondicionados	[N.2]	Daños por agua	4	2	8	16	4	2	8	9		
		[I.4]	Contaminación mecánica	4	5	20		2	3	7			
		[I.6]	Averías de origen físico o lógico	4	5	20		2	3	7			
		[E.15]	Errores en mantenimiento / Actualizacion de	3	5	16		3	5	13			

[power]	Fuentes de alimentación	[N.2]	Daños por agua	4	2	7	15	4	2	7	8
		[I.4]	Contaminación mecánica	4	5	18		2	3	7	
		[I.6]	Averías de origen físico o lógico	4	5	18		2	3	7	
		[E.15]	Errores en mantenimiento / Actualizacion de	3	5	15		3	5	12	
[gen]	Generadores eléctricos	[N.1]	Daños por fuego	5	2	10	18	5	2	10	11
		[N.2]	Daños por agua	5	2	10		5	2	10	
		[I.4]	Contaminación mecánica	5	5	25		3	3	9	
		[I.6]	Averías de origen físico o lógico	5	5	25		3	3	9	
		[E.15]	Errores en mantenimiento / Actualizacion de	4	5	20		4	5	16	
[prp.5]	Sistema de control biometrico dactila	[N.1]	Daños por fuego	5	2	9	14	5	2	9	9
		[N.2]	Daños por agua	5	2	9		5	2	9	
		[I.4]	Contaminación mecánica	4	5	19		2	3	7	
		[I.6]	Averías de origen físico o lógico	4	5	19		2	3	7	
		[I.8]	Condiciones inadecuadas	4	3	11		2	2	4	
		[I.10]	Interrupción de otros servicios y suministros	5	5	23		5	5	23	
		[E.15]	Errores en mantenimiento / Actualizacion de	4	4	15		2	2	5	
		[E.17]	Pérdida de equipos	2	4	9		2	4	8	
		[A.7]	Acceso no autorizado	4	3	11		3	3	9	
		[A.16]	Robo	5	4	19		4	4	15	
[furniture.1]	Stand Madera Oficinas	[N.1]	Daños por fuego	4	2	7	10	4	2	7	7
		[N.2]	Daños por agua	4	2	7		4	2	7	
		[N.3]	Desastres Naturales	4	2	7		2	1	3	
		[I.6]	Averías de origen físico o lógico	3	5	15		2	3	5	
		[I.8]	Condiciones inadecuadas	3	4	12		2	2	4	
		[E.15]	Errores en mantenimiento / Actualizacion de	3	4	12		2	3	8	
		[E.17]	Pérdida de equipos	2	4	7		2	4	6	
		[A.7]	Acceso no autorizado	2	5	9		2	5	7	
		[A.16]	Robo	4	4	15		3	4	12	
[furniture.2]	Stand Metálica Oficinas	[N.1]	Daños por fuego	4	2	7	14	4	2	7	9
		[N.2]	Daños por agua	5	2	10		5	2	10	
		[N.3]	Desastres Naturales	5	2	10		3	1	4	
		[I.6]	Averías de origen físico o lógico	4	5	20		2	3	7	
		[I.8]	Condiciones inadecuadas	4	5	20		2	3	7	
		[E.15]	Errores en mantenimiento / Actualizacion de	4	4	16		3	3	10	
		[E.17]	Pérdida de equipos	3	4	10		2	4	8	
		[A.7]	Acceso no autorizado	3	5	13		2	5	10	
		[A.16]	Robo	5	4	20		5	4	16	
[ups]	UPS Informática	[N.1]	Daños por fuego	4	2	8	15	4	2	8	10
		[N.2]	Daños por agua	4	2	8		4	2	8	
		[N.3]	Desastres Naturales	4	2	8		4	2	8	
		[I.4]	Contaminación mecánica	4	5	20		2	3	7	
		[I.6]	Averías de origen físico o lógico	4	5	20		2	3	7	
		[I.8]	Condiciones inadecuadas	4	4	16		2	2	6	
		[I.10]	Interrupción de otros servicios y suministros	4	5	20		4	5	20	
		[E.15]	Errores en mantenimiento / Actualizacion de	3	5	16		2	3	6	
		[E.17]	Pérdida de equipos	4	4	16		2	2	6	
		[A.7]	Acceso no autorizado	4	4	16		4	4	13	
		[A.16]	Robo	4	4	16		4	4	13	
		[A.17]	Ataque destructivo	4	4	16		4	4	13	

[PSTN]	Red telefónica	[I.9]	Falla de servicios de comunicaciones	3	4	12	12	3	4	12	10
		[E.2]	Errores de administrador	3	4	12		3	4	10	
		[E.7]	Errores de reencaminamiento	3	3	9		3	3	9	
		[E.8]	Errores de secuencia	2	3	7		2	2	5	
		[E.10]	Alteración accidental de información	2	5	12		2	4	8	
		[E.11]	Destruccion de información	3	5	15		2	3	5	
		[E.12]	Fugas de información	3	5	15		3	5	12	
		[E.16]	Caida de sistema por agotamiento de recurso	3	5	15		3	5	15	
		[A.9]	Intercepción de información	2	4	10		2	3	6	
		[A.10]	Modificación deliberada de información	3	4	12		3	4	10	
		[A.12]	Divulgación de información	3	4	12		3	4	10	
		[A.15]	Denegacion de Servicio	3	5	15		3	5	15	
COM	**Redes de Comunicaciones**										
[WAN]	Red de área amplia	[I.9]	Falla de servicios de comunicaciones	4	4	15	15	4	4	15	12
		[E.2]	Errores de administrador	4	4	15		3	4	12	
		[E.7]	Errores de reencaminamiento	4	3	11		4	3	11	
		[E.8]	Errores de secuencia	3	3	9		2	2	6	
		[E.10]	Alteración accidental de información	3	5	15		2	4	9	
		[E.11]	Destruccion de información	4	5	18		2	3	7	
		[E.12]	Fugas de información	4	5	18		3	5	15	
		[E.16]	Caida de sistema por agotamiento de recurso	4	5	18		4	5	18	
		[A.9]	Intercepción de información	3	4	12		2	3	8	
		[A.10]	Modificación deliberada de información	4	4	15		3	4	12	
		[A.12]	Divulgación de información	4	4	15		3	4	12	
		[A.15]	Denegacion de Servicio	4	5	18		4	5	18	
[LAN]	Red local	[I.9]	Falla de servicios de comunicaciones	4	4	16	16	4	4	16	13
		[E.2]	Errores de administrador	4	4	16		4	4	13	
		[E.7]	Errores de reencaminamiento	4	3	12		4	3	12	
		[E.8]	Errores de secuencia	3	3	10		3	2	6	
		[E.10]	Alteración accidental de información	3	5	16		3	4	10	
		[E.11]	Destruccion de información	4	5	20		2	3	7	
		[E.12]	Fugas de información	4	5	20		4	5	16	
		[E.16]	Caida de sistema por agotamiento de recurso	4	5	20		4	5	20	
		[A.9]	Intercepción de información	3	4	13		3	3	8	
		[A.10]	Modificación deliberada de información	4	4	16		4	4	13	
		[A.12]	Divulgación de información	4	4	16		4	4	13	
		[A.15]	Denegacion de Servicio	4	5	20		4	5	20	
[wifi]	Wifi	[I.9]	Falla de servicios de comunicaciones	3	4	13	14	3	4	13	11
		[E.2]	Errores de administrador	3	4	13		3	4	11	
		[E.7]	Errores de reencaminamiento	3	3	10		3	3	10	
		[E.8]	Errores de secuencia	3	3	8		2	2	5	
		[E.10]	Alteración accidental de información	3	5	13		2	4	9	
		[E.11]	Destruccion de información	3	5	17		2	3	6	
		[E.12]	Fugas de información	3	5	17		3	5	14	
		[E.16]	Caida de sistema por agotamiento de recurso	3	5	17		3	5	17	
		[A.9]	Intercepción de información	3	4	11		2	3	7	
		[A.10]	Modificación deliberada de información	3	4	13		3	4	11	
		[A.12]	Divulgación de información	3	4	13		3	4	11	
		[A.15]	Denegacion de Servicio	3	5	17		3	5	17	

L	Instalaciones											
[building.1]	Edificio Clinica	[N.1]	Daños por fuego	4	2	7	12	2	1	3	9
		[N.2]	Daños por agua	4	2	7		4	2	7	
		[N.3]	Desastres Naturales	4	2	7		4	2	7	
		[E.10]	Alteración accidental de información	3	5	15		2	4	9	
		[E.11]	Destruccion de información	3	5	15		2	4	9	
		[A.7]	Acceso no autorizado	4	5	18		3	5	15	
		[A.17]	Ataque destructivo	3	5	15		3	5	12	
		[A.18]	Ocupación enemiga	4	3	11		3	3	9	
[building.2]	Edificio Torre Nueva	[N.1]	Daños por fuego	3	2	6	10	2	1	2	7
		[N.2]	Daños por agua	3	2	6		3	2	6	
		[N.3]	Desastres Naturales	3	2	6		3	2	6	
		[E.10]	Alteración accidental de información	2	5	12		2	4	8	
		[E.11]	Destruccion de información	2	5	12		2	4	8	
		[A.7]	Acceso no autorizado	3	5	15		3	5	12	
		[A.17]	Ataque destructivo	2	5	12		2	5	10	
		[A.18]	Ocupación enemiga	3	3	9		3	3	7	
[local.1]	Oficinas 1 piso	[N.1]	Daños por fuego	4	2	8	13	4	2	8	10
		[N.2]	Daños por agua	4	2	8		4	2	8	
		[N.3]	Desastres Naturales	4	2	8		4	2	8	
		[E.10]	Alteración accidental de información	3	5	16		3	4	10	
		[E.11]	Destruccion de información	3	5	16		2	3	6	
		[A.7]	Acceso no autorizado	4	5	20		4	5	16	
		[A.10]	Modificación deliberada de información	3	5	16		3	5	13	
		[A.11]	Destrucción de información	3	5	16		2	3	6	
		[A.12]	Divulgación de información	2	5	10		2	5	8	
		[A.17]	Ataque destructivo	3	5	16		3	5	13	
		[A.18]	Ocupación enemiga	4	3	12		4	3	10	

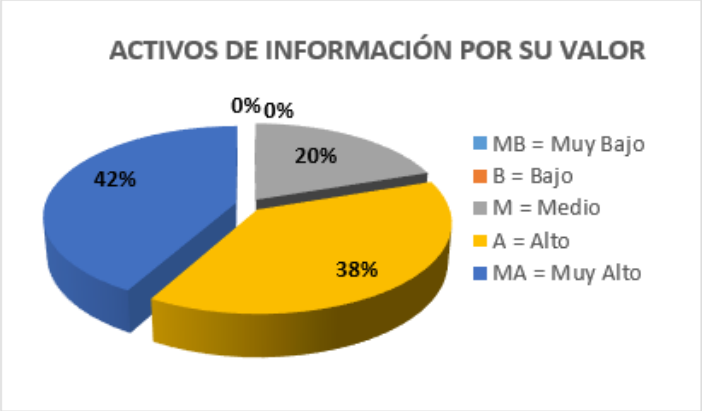
[local.2]	Oficinas 2 piso	[N.1]	Daños por fuego	4	2	8	13	4	2	8	10
		[N.2]	Daños por agua	4	2	8		4	2	8	
		[N.3]	Desastres Naturales	4	2	8		4	2	8	
		[E.10]	Alteración accidental de información	3	5	16		3	4	10	
		[E.11]	Destruccion de información	3	5	16		2	3	6	
		[A.7]	Acceso no autorizado	4	5	20		4	5	16	
		[A.10]	Modificación deliberada de información	3	5	16		3	5	13	
		[A.11]	Destrucción de información	3	5	16		2	3	6	
		[A.12]	Divulgación de información	2	5	10		2	5	8	
		[A.17]	Ataque destructivo	3	5	16		3	5	13	
		[A.18]	Ocupación enemiga	4	3	12		4	3	10	
[local.3]	Oficinas 3 piso	[N.1]	Daños por fuego	4	2	8	13	4	2	8	10
		[N.2]	Daños por agua	4	2	8		4	2	8	
		[N.3]	Desastres Naturales	4	2	8		4	2	8	
		[E.10]	Alteración accidental de información	3	5	16		3	4	10	
		[E.11]	Destruccion de información	3	5	16		2	3	6	
		[A.7]	Acceso no autorizado	4	5	20		4	5	16	
		[A.10]	Modificación deliberada de información	3	5	16		3	5	13	
		[A.11]	Destrucción de información	3	5	16		2	3	6	
		[A.12]	Divulgación de información	2	5	10		2	5	8	
		[A.17]	Ataque destructivo	3	5	16		3	5	13	
		[A.18]	Ocupación enemiga	4	3	12		4	3	10	
[local.4]	Sector Consultorios Medicos Clinica	[N.1]	Daños por fuego	3	2	6	10	3	2	6	7
		[N.2]	Daños por agua	3	2	6		3	2	6	
		[N.3]	Desastres Naturales	3	2	6		3	2	6	
		[E.10]	Alteración accidental de información	2	5	12		2	4	8	
		[E.11]	Destruccion de información	2	5	12		1	3	4	
		[A.7]	Acceso no autorizado	3	5	15		3	5	12	
		[A.10]	Modificación deliberada de información	2	5	12		2	5	10	
		[A.11]	Destrucción de información	2	5	12		1	3	4	
		[A.12]	Divulgación de información	2	5	8		1	5	6	
		[A.17]	Ataque destructivo	2	5	12		2	5	10	
		[A.18]	Ocupación enemiga	3	3	9		3	3	7	
[local.5]	Sector Consultorios Medicos Torre Nueva	[N.1]	Daños por fuego	3	2	7	11	3	2	7	8
		[N.2]	Daños por agua	3	2	7		3	2	7	
		[N.3]	Desastres Naturales	3	2	7		3	2	7	
		[E.10]	Alteración accidental de información	3	5	13		2	4	9	
		[E.11]	Destruccion de información	3	5	13		2	3	5	
		[A.7]	Acceso no autorizado	3	5	17		3	5	14	
		[A.10]	Modificación deliberada de información	3	5	13		2	5	11	
		[A.11]	Destrucción de información	3	5	13		2	3	5	
		[A.12]	Divulgación de información	2	5	8		2	5	7	
		[A.17]	Ataque destructivo	3	5	13		2	5	11	
		[A.18]	Ocupación enemiga	3	3	10		3	3	8	
[local.6]	Sector Historias Clinicas	[N.1]	Daños por fuego	4	2	8	13	4	2	8	9
		[N.2]	Daños por agua	4	2	8		4	2	8	
		[N.3]	Desastres Naturales	4	2	8		4	2	8	
		[E.10]	Alteración accidental de información	3	5	16		3	4	10	
		[E.11]	Destruccion de información	3	5	16		2	3	6	
		[A.7]	Acceso no autorizado	4	5	20		4	5	16	
		[A.11]	Destrucción de información	3	5	16		2	3	6	
		[A.12]	Divulgación de información	2	5	10		2	5	8	
		[A.17]	Ataque destructivo	3	5	16		3	5	13	
		[A.18]	Ocupación enemiga	4	3	12		4	3	10	

[local.7]	Sector Informatica	[N.1]	Daños por fuego	5	2	10	20	5	2	10	15		
		[N.2]	Daños por agua	5	2	10		5	2	10			
		[N.3]	Desastres Naturales	5	2	10		5	2	10			
		[E.10]	Alteración accidental de información	5	5	25		5	5	25			
		[E.11]	Destruccion de información	5	5	25		3	3	9			
		[A.7]	Acceso no autorizado	5	5	25		5	5	20			
		[A.10]	Modificación deliberada de información	5	5	25		5	5	20			
		[A.11]	Destrucción de información	4	5	20		2	3	7			
		[A.12]	Divulgación de información	5	5	25		5	5	20			
		[A.17]	Ataque destructivo	5	5	25		5	5	20			
		[A.18]	Ocupación enemiga	5	3	15		5	3	12			
P	Personal												
[ui.1]	Administrativos General	[E.5]	Deficiencias de la organización	3	5	17	15	3	5	14	12		
		[E.12]	Fugas de información	3	4	14		3	4	11			
		[E.18]	Indisponibilidad del personal	3	4	14		3	4	11			
		[A.19]	Indisponibilidad del personal	4	5	22		4	5	18			
[ui.2]	Gerencia Administrativa	[E.5]	Deficiencias de la organización	4	5	20	19	4	5	16	16		
		[E.12]	Fugas de información	4	4	16		4	4	13			
		[E.18]	Indisponibilidad del personal	4	4	16		4	4	13			
		[A.19]	Indisponibilidad del personal	5	5	25		5	5	20			
[ui.3]	Jefaturas	[E.5]	Deficiencias de la organización	4	5	20	19	4	5	16	16		
		[E.12]	Fugas de información	4	4	16		4	4	13			
		[E.18]	Indisponibilidad del personal	4	4	16		4	4	13			
		[A.19]	Indisponibilidad del personal	5	5	25		5	5	20			
[adm]	Administradores de sistemas	[E.5]	Deficiencias de la organización	4	5	20	19	4	5	16	16		
		[E.12]	Fugas de información	4	4	16		4	4	13			
		[E.18]	Indisponibilidad del personal	4	4	16		4	4	13			
		[A.19]	Indisponibilidad del personal	5	5	25		5	5	20			
[des]	Desarrolladores/programadores	[E.5]	Deficiencias de la organización	4	5	20	19	4	5	16	16		
		[E.12]	Fugas de información	4	4	16		4	4	13			
		[E.18]	Indisponibilidad del personal	4	4	16		4	4	13			
		[A.19]	Indisponibilidad del personal	5	5	25		5	5	20			
[ui.4]	Personal Asistencial, Ténicos y Laboratoristas	[E.5]	Deficiencias de la organización	3	5	15	14	3	5	12	11		
		[E.12]	Fugas de información	3	4	12		3	4	10			
		[E.18]	Indisponibilidad del personal	3	4	12		3	4	10			
		[A.19]	Indisponibilidad del personal	4	5	18		3	5	15			
[ui.5]	Personal de Auditoria Medica	[E.5]	Deficiencias de la organización	3	5	16	15	3	5	13	12		
		[E.12]	Fugas de información	3	4	13		3	4	10			
		[E.18]	Indisponibilidad del personal	3	4	13		3	4	10			
		[A.19]	Indisponibilidad del personal	4	5	20		4	5	16			
[ui.6]	Personal Hist Clinicas	[E.5]	Deficiencias de la organización	3	5	15	14	3	5	12	11		
		[E.12]	Fugas de información	3	4	12		3	4	10			
		[E.18]	Indisponibilidad del personal	3	4	12		3	4	10			
		[A.19]	Indisponibilidad del personal	4	5	18		3	5	15			

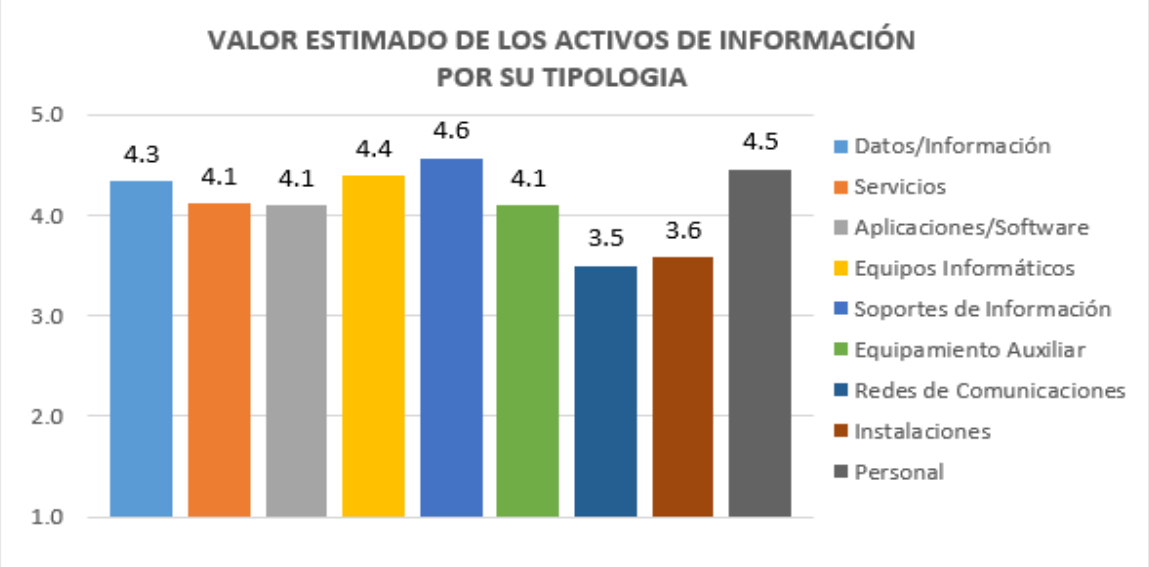
Este es el análisis de riesgos de los activos de información que se realizó a la Clínica Internacional –Piura, para conocer la situación actual en la que se encontraba. A continuación en el apartado siguiente se mostraran algunos resultados, obtenidos de la investigación.

PAR 3.-Comunicación de Resultados.

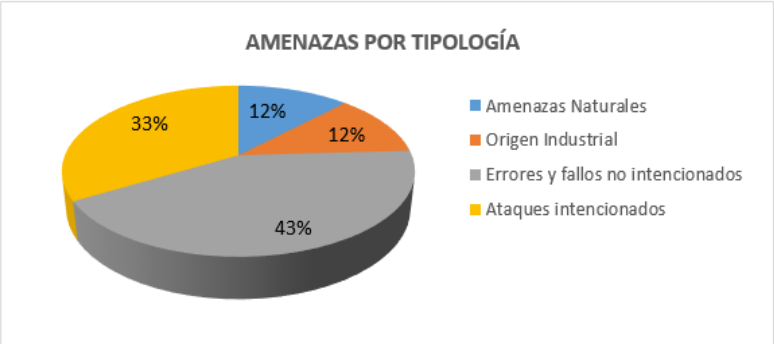
- **Activos de Información por nivel:** Se muestra que los activos de información en conjunto se encuentran en un nivel alto de valoración.



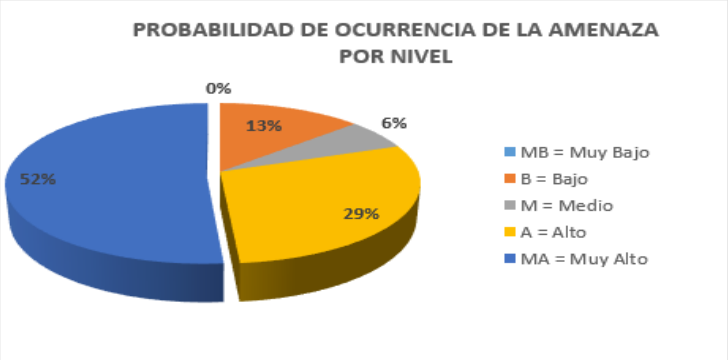
- **Tipos de activo por valoración:** Se muestra que tipos de activos son los que poseen más valor para la organización, en este caso soportes de información



- **Amenazas por tipología:** Se muestra que los tipos de amenazas a los que está más expuesta la organización son los de origen errores y fallos no intencionados y también los ataquen intencionados.

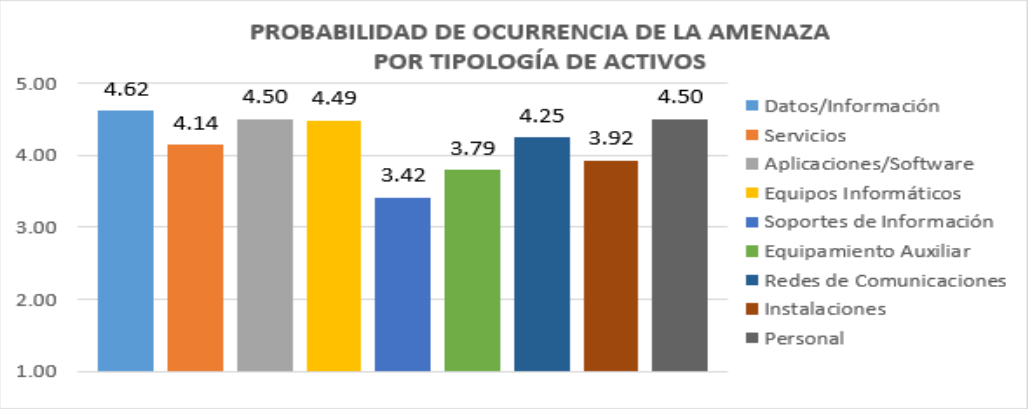


- **Probabilidad de las amenazas por nivel:** Se muestra que las amenazas se encuentran en una probabilidad de ocurrencia muy alta.

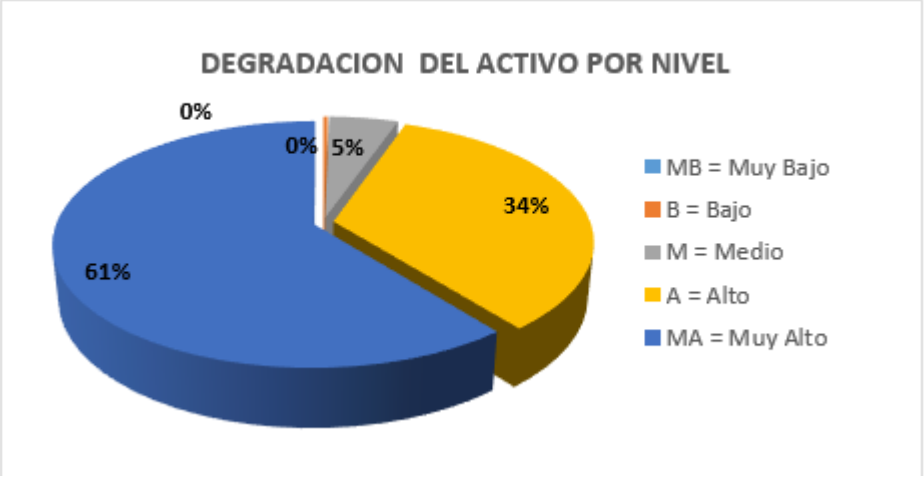


-

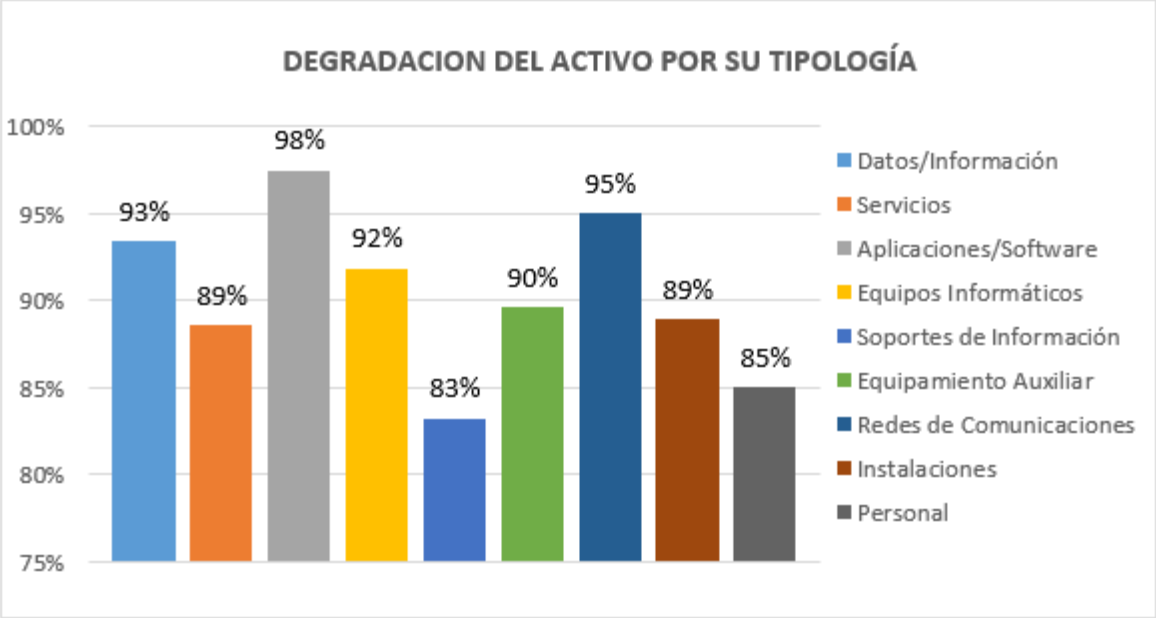
- **Probabilidad de las amenazas por tipo de activo:** Se muestra que los tipos de activos más afectados por si se dan las amenazas son los datos / información.



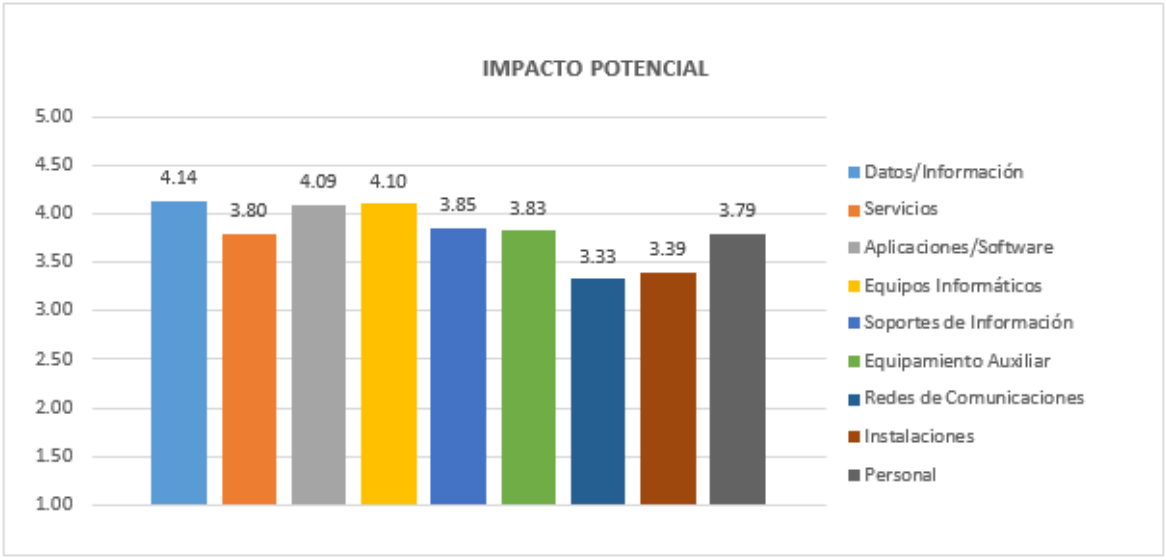
- **Degradación de los activos por nivel:** Como resultado del análisis se obtiene que los tipos de activos en su mayoría tienen una degradación muy alta, esto quiere decir que, los activos de información pueden sufrir grandes pérdidas en relación a su valor.



- **Degradación de los activos por tipo de activo:** Se muestra que los tipos de activos aplicaciones y software tienen una degradación muy alta.

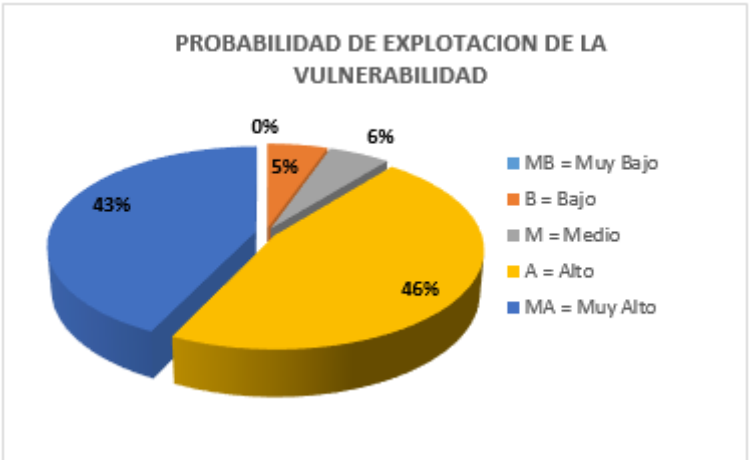


- **Impacto potencial por tipo de activo:** Se muestra que los tipos de activos que tienen un impacto mayor son los de Datos/ Información.

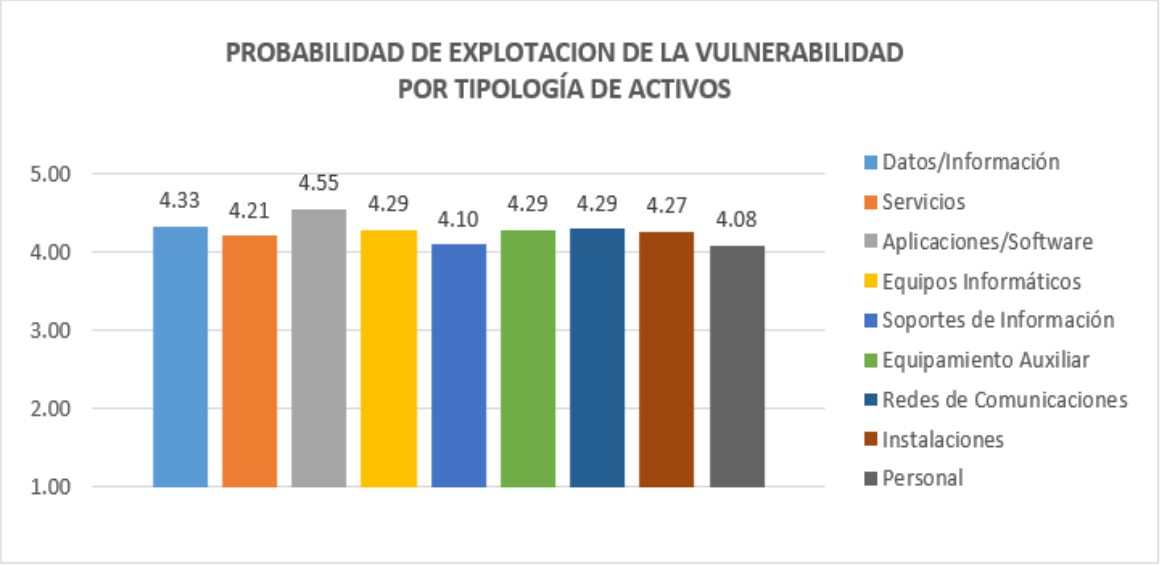


- **Se obtiene el riesgo potencial por tipo de activo**: Se muestra que los muchos de los tipos de activos que la organización posee, tienen un riesgo mayor.

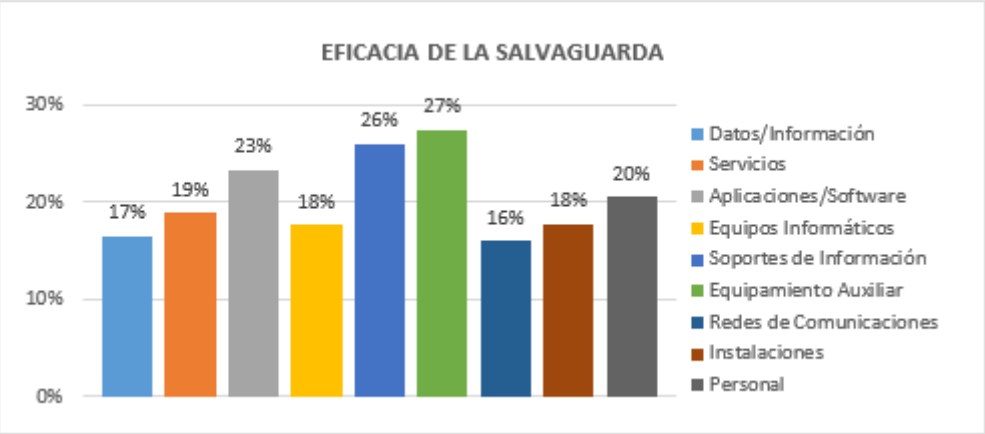
- **Probabilidad de explotación de las vulnerabilidades por nivel**: Se muestra que las vulnerabilidades se encuentran en una probabilidad muy alta de que sean explotadas por las amenazas.



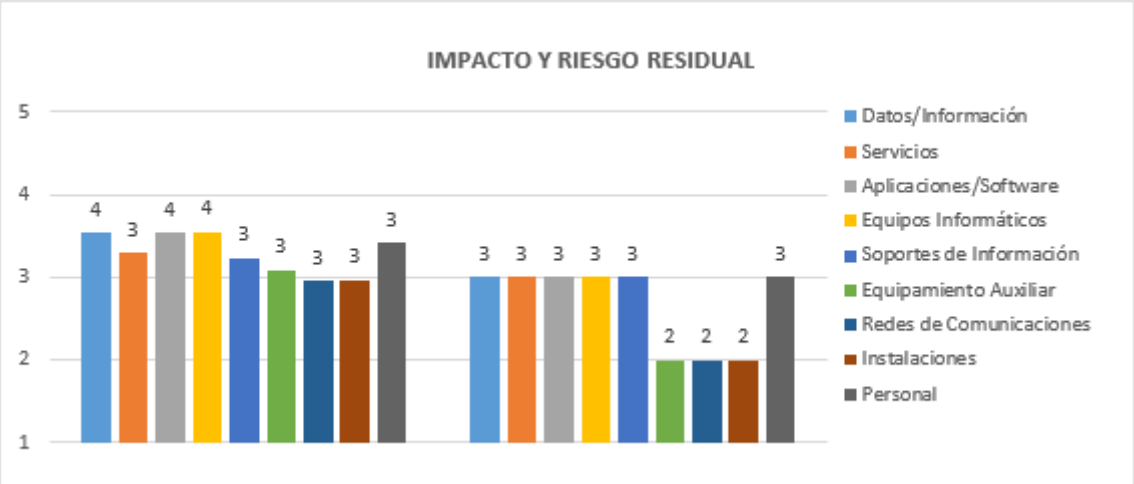
- **Probabilidad de las vulnerabilidades por tipo de activo**: Se muestra que los tipos de activos más afectados por si las amenazas explotan las vulnerabilidades son los de tipo aplicaciones/software seguido de datos/ información.



- **Se obtiene la eficacia de la salvaguarda por tipo de activo**: Se muestra que la mayoría de los tipos de activos tienen una eficacia entre el 0% y 40%.



- **Se obtiene el impacto y riesgo residual por tipo de activo**: Se muestra que los tipos de activos en su mayoría tienen un impacto y riesgo entre un nivel medio y un nivel alto con las salvaguardas actuales.



- **Tratamiento de riesgos residuales**

Opciones de Tratamiento de riesgo residual

Riesgo Muy Bajo Valor 1 - 5 Asumir Riesgo	Riesgo Bajo Valor 6 - 10 Administrar Riesgo	Riesgo Medio Valor 11 -15 Reducir el riesgo a niveles bajos	Riesgo Alto Valor 16 - 20 Evitar - Gestionar el Riesgo	Riesgo Muy Alto Valor 21 - 25 Evitar - Gestionar el Riesgo Requiere accion inmediata

Cod	Amenazas	Tipo de Activo Afectado	RR	Riesgo Residual	Opción de Tratamiento	Salvaguarda	Descripcion de Plan de Accion	Responsable
[A.1]	Manipulación de los registros de actividad (log)	Datos/Información	12	Riesgo Medio	Reducir el riesgo a niveles bajos	Herramienta para análisis de logs	Monitorear periódica los Logs de eventos de seguridad.	Area de TI
[A.10]	Modificación deliberada de información	Datos/Información Servicios Aplicaciones/Software Soportes de Información Redes de Comunicaciones Instalaciones	9	Riesgo Bajo	Administrar Riesgo	Politicas de Seguridad de accesos lógicos	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema	Area de TI
[A.11]	Destrucción de información	Datos/Información Servicios Aplicaciones/Software Soportes de Información Instalaciones	10	Riesgo Bajo	Administrar Riesgo	Se aplican perfiles de seguridad	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Area de TI
[A.12]	Divulgación de información	Datos/Información Servicios Aplicaciones/Software Soportes de Información Redes de Comunicaciones Instalaciones	13	Riesgo Medio	Reducir el riesgo a niveles bajos	Control de los accesos físicos	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Area de TI
[A.14]	Manipulacion de Equipos	Equipos Informáticos Soportes de Información Equipamiento Auxiliar Instalaciones	15	Riesgo Medio	Reducir el riesgo a niveles bajos	Identificación y autenticación	Garantizar que este implementada la política de contraseña segura	Area de TI
[A.15]	Denegacion de Servicio	Datos/Información Servicios Aplicaciones/Software Equipos Informáticos Soportes de Información Equipamiento Auxiliar Redes de Comunicaciones	13	Riesgo Medio	Reducir el riesgo a niveles bajos	Protección del servidor de nombres de dominio (DNS)	Garantizar la debida ejecución de las pruebas de contingencia de TI	Area de TI
[A.16]	Robo	Equipos Informáticos Soportes de Información Equipamiento Auxiliar	16	Riesgo Alto	Evitar - Gestionar el Riesgo	Control de los accesos físicos	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Area de TI
[A.17]	Ataque destructivo	Soportes de Información Equipamiento Auxiliar Redes de Comunicaciones Instalaciones	15	Riesgo Medio	Reducir el riesgo a niveles bajos	Politicas de Seguridad Física	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Area de TI
[A.18]	Ocupación enemiga	Instalaciones	9	Riesgo Bajo	Administrar Riesgo	Control de los accesos físicos	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Area de TI
[A.19]	Indisponibilidad del personal	Personal	15	Riesgo Medio	Reducir el riesgo a niveles bajos	Formacion y Concientizacion	Garantizar que este implementada la política de contraseña segura	Area de TI
[A.2]	Manipulación de la configuración	Datos/Información	22	Riesgo Muy Alto	Evitar - Gestionar el Riesgo Requiere accion inmediata	Identificación y autenticación	Garantizar la implementación del bloqueo de dispositivos externos en los computadores de la entidad	Area de TI

[A.3]	Suplantación de identidad	Datos/Información Servicios Aplicaciones/Software Redes de Comunicaciones	3	Riesgo Muy Bajo	Asumir Riesgo	Cifrado de la información	Garantizar que este implementada la politica de contraseña segura	Area de TI
[A.4]	Abuso de privilegios de acceso	Datos/Información Servicios Aplicaciones/Software Equipos Informáticos Redes de Comunicaciones	12	Riesgo Medio	Reducir el riesgo a niveles bajos	Se aplican perfiles de seguridad	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Area de TI
[A.5]	Uso no previsto	Servicios Aplicaciones/Software Equipos Informáticos Soportes de Información Equipamiento Auxiliar Instalaciones	16	Riesgo Alto	Evitar - Gestionar el Riesgo	Formacion y Concientizacion	itación del personalRealizar permanentemer	Area de TI
[A.7]	Acceso no autorizado	Datos/Información Servicios Aplicaciones/Software Equipos Informáticos Soportes de Información Equipamiento Auxiliar Redes de Comunicaciones Instalaciones	14	Riesgo Medio	Reducir el riesgo a niveles bajos	Control de los accesos físicos	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Area de TI
[A.8]	Repudio	Datos/Información Servicios	2	Riesgo Muy Bajo	Asumir Riesgo	Formacion y Concientizacion	Garantizar la debida capacitación del personal Realizar permanentemente campañas de seguridad	Area de TI
[A.9]	Intercepción de información	Redes de Comunicaciones	7	Riesgo Bajo	Administrar Riesgo	Politicas de Continuidad de la seguridad de la información. Cifrado de la información	Garantizar la debida ejecución de las pruebas de continuidad	Area de TI
[E.1]	Errores de usuarios	Datos/Información Servicios Aplicaciones/Software Soportes de Información	21	Riesgo Muy Alto	Evitar - Gestionar el Riesgo Requiere accion inmediata	Formacion y Concientizacion	Garantizar la debida capacitación del personal Realizar permanentemente campañas de seguridad	Area de TI
[E.10]	Alteración accidental de información	Datos/Información Servicios Aplicaciones/Software Soportes de Información Redes de Comunicaciones Instalaciones	9	Riesgo Bajo	Administrar Riesgo	Formacion y Concientizacion	Garantizar la debida capacitación del personal Realizar permanentemente campañas de seguridad	Area de TI
[E.11]	Destruccion de información	Datos/Información Servicios Aplicaciones/Software Soportes de Información Redes de Comunicaciones Instalaciones	11	Riesgo Medio	Reducir el riesgo a niveles bajos	Formacion y Concientizacion Copias de seguridad de los datos (backup)	Garantizar la debida capacitación del personal Realizar permanentemente campañas de seguridad	Area de TI
[E.12]	Fugas de información	Datos/Información Servicios Aplicaciones/Software Soportes de Información Redes de Comunicaciones Instalaciones Personal	12	Riesgo Medio	Reducir el riesgo a niveles bajos	Politicas de seguridad logica Politicas ligadas a los recursos humanos	Garantizar que este implementada las políticas de contraseña segura y bloqueo automático de pantallas. Realizar permanentemente campañas de seguridad Acuerdos de confidencialidad	Area de TI
[E.14]	Errores en mantenimiento / Actualizacion de software	Aplicaciones/Software	14	Riesgo Medio	Reducir el riesgo a niveles bajos	Se aplican perfiles de seguridad	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Area de TI
[E.15]	Errores en mantenimiento / Actualizacion de equipos	Datos/Información Servicios Aplicaciones/Software Equipos Informáticos Soportes de Información Equipamiento Auxiliar Redes de Comunicaciones Instalaciones Personal	11	Riesgo Medio	Reducir el riesgo a niveles bajos	Se aplican perfiles de seguridad	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Area de TI
[E.16]	Caida de sistema por agotamiento de recursos.	Servicios Equipos Informáticos Redes de Comunicaciones	20	Riesgo Alto	Evitar - Gestionar el Riesgo	Formacion y Concientizacion	Garantizar la debida capacitación del personal Realizar permanentemente campañas de seguridad	Area de TI
[E.17]	Pérdida de equipos	Equipos Informáticos Soportes de Información Equipamiento Auxiliar	12	Riesgo Medio	Reducir el riesgo a niveles bajos	Politicas de Clasificación de la información.	inventarias los activos de iinformacion	Area de TI
[E.2]	Errores de administrador	Datos/Información Servicios Aplicaciones/Software Equipos Informáticos Soportes de Información Redes de Comunicaciones	13	Riesgo Medio	Reducir el riesgo a niveles bajos	Politicas de Responsabilidades y procedimientos de operación Segregacion de tareas	Monitorear periódica los Logs de eventos de seguridad Garantizar la debida capacitación del personal de TI Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios	Area de TI

[E.3]	Errores de Monitorización	Datos/Información	22	Riesgo Muy Alto	Evitar - Gestionar el Riesgo Requiere accion inmediata	DLP: Herramienta de monitorización de contenidos	Monitorear periódica los Logs de eventos de seguridad	Area de TI
[E.4]	Errores de Configuración	Datos/Información	12	Riesgo Medio	Reducir el riesgo a niveles bajos	Herramienta de chequeo de configuración Herramienta para análisis de logs Politicas de Responsabilidades y procedimientos de operación	Monitorear periódica los Logs de eventos de seguridad. Documentar la iformacion de los sistemas.	Area de TI
[E.5]	Deficiencias de la organización	Personal	14	Riesgo Medio	Reducir el riesgo a niveles bajos	Politicas de Seguridad Física	Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Area de TI
[E.6]	Disfusión de software dañino	Aplicaciones/Software	12	Riesgo Medio	Reducir el riesgo a niveles bajos	Control de acceso lógico	Revisar periódicamente la efectividad de la solución de anti spam	Area de TI
[E.7]	Errores de reencaminamiento	Servicios Aplicaciones/Software Redes de Comunicaciones	11	Riesgo Medio	Reducir el riesgo a niveles bajos			Area de TI
[E.8]	Errores de secuencia	Aplicaciones/Software Equipos Informáticos Redes de Comunicaciones	7	Riesgo Bajo	Administrar Riesgo	Protección del correo electrónico	Implementar mecanismos que garanticen el cifrado de la información que se intercambia con terceros a través del correo electrónico	Area de TI
[I.10]	Interrupción de otros servicios y suministros esenciales	Equipamiento Auxiliar	22	Riesgo Muy Alto	Evitar - Gestionar el Riesgo Requiere accion inmediata	Politicas de Continuidad de la seguridad de la información.	Garantizar la debida ejecución de las pruebas de continuidad	Area de TI
[I.11]	Degradación de los soportes de almacenamiento de la información	Soportes de Información Equipamiento Auxiliar Redes de Comunicaciones Instalaciones Personal	10	Riesgo Bajo	Administrar Riesgo	Politicas de Continuidad de la seguridad de la información.	Garantizar la debida ejecución de las pruebas de continuidad	Area de TI
[I.4]	Contaminación mecánica	Equipos Informáticos Soportes de Información Equipamiento Auxiliar	7	Riesgo Bajo	Administrar Riesgo	Protección de las Instalaciones	Garantizar la implementación del bloqueo de dispositivos externos en los computadores de la entidad	Area de TI
[I.6]	Averías de origen físico o lógico	Aplicaciones/Software Equipos Informáticos Soportes de Información Equipamiento Auxiliar	11	Riesgo Medio	Reducir el riesgo a niveles bajos	Cambios (actualizaciones y mantenimiento)	Adecuados mantenimientos preventivos y correctivos	Area de TI
[I.7]	Corte de suministro eléctrico	Equipos Informáticos Soportes de Información Equipamiento Auxiliar	13	Riesgo Medio	Reducir el riesgo a niveles bajos	Suministro eléctrico	Garantizar la debida ejecución de las pruebas de contingencia de TI	Area de TI
[I.8]	Condiciones inadecuadas de temperatura o humedad	Equipos Informáticos Soportes de Información Equipamiento Auxiliar	6	Riesgo Bajo	Administrar Riesgo	Climatización Instalación	Garantizar la debida ejecución de las pruebas de continuidad	Area de TI
[I.9]	Falla de servicios de comunicaciones	Redes de Comunicaciones	14	Riesgo Medio	Reducir el riesgo a niveles bajos	Conexiones de red pública desprotegidas Fallo del sistema Insuficiente mantenimiento / mala instalación de los	Implantación de solución en alta disponibilidad para aquellos servicios críticos	Area de TI
[N.1]	Daños por fuego	Equipos Informáticos Soportes de Información Equipamiento Auxiliar Instalaciones	8	Riesgo Bajo	Administrar Riesgo	Plan de Recuperación de Desastres (DRP)	Garantizar la debida ejecución de las pruebas de continuidad	Coordiador de plan de continuidad
[N.2]	Daños por agua	Equipos Informáticos Soportes de Información Equipamiento Auxiliar Instalaciones	9	Riesgo Bajo	Administrar Riesgo	Plan de Recuperación de Desastres (DRP)	Garantizar la debida ejecución de las pruebas de continuidad	Coordiador de plan de continuidad
[N.3]	Desastres Naturales	Equipos Informáticos Soportes de Información Equipamiento Auxiliar Instalaciones	8	Riesgo Bajo	Administrar Riesgo	Plan de Recuperación de Desastres (DRP)	Garantizar la debida ejecución de las pruebas de continuidad	Coordiador de plan de continuidad

Anexo N°18 **Plan de Seguridad**

CLINICA INTERNACIONAL – PIURA

PLAN DE SEGURIDAD DE LA INFORMACION

Plan de seguridad (PS)

1. Introducción

Este plan de seguridad de la información es una propuesta elaborada como respuesta a los resultados obtenidos del análisis de riesgos de los activos de información de Clínica Internacional – Piura. Este plan está conformado por una serie de proyectos pensados realizar en un lapso de 2 años, cuya programación se verá posteriormente en los siguientes apartados.

Los proyectos escogidos están basados en diferentes indagaciones encontradas a lo largo de toda la investigación adecuándolos a los resultados obtenidos con el análisis de riesgos, lo que permitió poder enlazar el listado de salvaguardas que brinda la metodología aplicada (MAGERIT), con los controles y/o políticas que brinda la ISO/IEC 27002:2013, es importante destacar esto, puesto que se definen las salvaguardas principales determinadas en el análisis de riesgos que tienen relación con los proyectos definidos, lo cual permite poder en un futuro analizar el riesgo residual ya basado en las salvaguardas que involucran la implementación de dichos proyectos y poder definir su eficacia sobre los activos de información, y conocer como se encuentra la situación de la organización.

1.1 Propósito del Plan

El propósito que tiene esta propuesta es identificar y describir los proyectos de seguridad de la información que necesita la organización para salvaguardar los activos en riesgo, en base a distintas investigaciones, además de brindar a la organización el cumplimiento efectivo de los controles que brinda la ISO/IEC27002:2013, y se vaya preparando para una futura certificación, lo mismo que sería beneficioso para toda entidad y lo que se espera de esta organización.

PS 1.- Identificación de proyectos de seguridad.

ID:	**DOC - 01**
Nombre Propuesta:	**Política de Seguridad**
Tipo:	**Documentación**

Detalles

Descripción del proyecto a realizar:

Es necesario e importante crear un documento de políticas de seguridad que especifiquen los requisitos de la organización en relación a la seguridad de los activos de información, el mismo que será revisado y actualizado previo acuerdo, en un lapso de tiempo determinado por la organización, ya que existirán cambios constantes que deberán ser agregados o modificados según sea el caso.

Dicho documento estará a disposición del personal de la organización, asimismo deberá cumplirse y respetarse. El mismo contendrá las sanciones correspondientes por incumplimiento.

Salvaguardas y/o controles principales:

- Políticas de accesos.
- Políticas de Responsabilidades y procedimientos de operación
- Políticas de clasificación de la información
- Políticas ligadas a los recursos humanos, entre otras políticas.

Tareas:

- Creación de un manual de políticas, que brinde las pautas necesarias para salvaguardar a los activos de información.
- Estandarizar las políticas de seguridad a la norma ISO27002.
- Especificaciones, de los usuarios, como:
  - Controles adecuados.
  - Responsabilidades y roles definidos en relación a la seguridad.
- Formación y Concientización

Beneficios:

- Disminución de riesgos, saber cómo prevenir el riesgo.
- Conocimiento de controles.
- Grado de adaptación.

Responsable: Área de TI

Dominio ISO relacionado	**5.1.1 Conjunto de políticas para la seguridad de la información.** **5.1.2 Revisión de las políticas para la seguridad de la información**
Activos del AARR afectados	**El conjunto de todos los activos de la organización**
Amenazas Afrontadas	**Intencionales, No intencionales, Naturales, Industrial**
Tiempo estimado	**2 Meses – Corto Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 500.00**

ID:	**DOC - 02**
Nombre Propuesta:	**Plan de continuidad de negocio**

Tipo:	Documentación

Detalles

Descripción del proyecto a realizar:

Creación de un documento, para respaldar a los activos de información sobre todo a las operaciones de la organización, permitiéndole estar preparados ante distintos acontecimientos que ponen en peligro la continuidad de las operaciones y se sepa afrontar a las posibles amenazas que puedan darse.

Este documento, será revisado al igual que el DOC - 01 de forma periódica y a cargo de las personas responsables.

Salvaguardas y/o controles principales:

- Planificación de la seguridad
- Inspecciones de seguridad

Tareas:

- Detallar el plan de continuidad del negocio.
- Dar el debido control al plan.
- Conocimiento para estar preparado ante distintas eventualidades producidos por las diferentes amenazas a las que la organización está expuesta.

Beneficios:

- Minimización de los riesgos.
- Estar prevenido ante diferentes dificultades.(Continuidad de las Operaciones)

Responsable: Área de TI

Dominio ISO relacionado	**14.1 Aspectos de la gestión de continuidad de negocio**
Activos del AARR afectados	**El conjunto de todos los activos de la organización**
Amenazas Afrontadas	**Intencionales, No intencionales, Naturales, Industrial**
Tiempo estimado	**6 Meses – Mediano Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 1,500.00**

ID:	**DOC - 03**
Nombre Propuesta:	**Mantenimiento de sistemas**
Tipo:	**Documentación**

Detalles

Descripción del proyecto a realizar:

Es necesario tener un plan plasmado en un documento, donde se especifiquen, cada una de los requerimientos que tiene la organización en relación al mantenimiento de los sistemas de información.

Dicho documento debe contener distintas características que permitirán tener un control del funcionamiento y el mantenimiento de sistemas, sabiendo que tipo de mantenimiento debe darse y cada qué período. Asimismo, identificar las distintas medidas para su protección y uso correspondiente.

Cabe resaltar que al igual que los demás documentos planteados anteriormente, se debe revisar y actualizar según los cambios que se den en la organización

Salvaguardas y/o controles principales:

- Cambios (actualizaciones y mantenimiento)
- Aseguramiento de la disponibilidad

Tareas:

- Elaboración de manuales de usuario de sistemas de información
- Elaboración de un documento que incluya la data necesaria sobre los sistemas y sus actualizaciones.
- Lista de medidas para la protección de los activos de información.
- Documentación por parte del personal a cargo de los mantenimientos

Beneficios:

- Buen uso y mantenimiento de los sistemas de información
- Reducción de riesgos en relación a las vulnerabilidades de desconocimiento en sistemas de información y errores de usuarios.

Responsable: Área de TI

Dominio ISO relacionado	**7.1 Responsabilidad sobre los activos** **9.2 Seguridad de los equipos**
Activos del AARR afectados	**El conjunto de todos los activos de la organización**
Amenazas Afrontadas	**Intencionales, No intencionales, Naturales, Industrial**
Tiempo estimado	**3 Meses – Corto Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 1,000.00**

ID:	**DOC - 04**
Nombre Propuesta:	**Gestión de Activos**
Tipo:	**Documentación**

Detalles

Descripción del proyecto a realizar:

Es necesario documentar los activos que posee la organización, clasificándolos según tipología (datos/información, servicios, aplicaciones/software, equipos informáticos, soportes de información, equipamiento auxiliar, redes de comunicaciones, instalaciones y personal), agregando una breve descripción del activo, cuál es su funcionalidad, el área al que pertenece, usuario que lo utiliza, entre otros aspecto que se deban considerar.

Este documento tendrá una revisión periódica, para su actualización, o adición de nuevos activos de información.

Salvaguardas y/o controles principales:

- Gestión de Activos

Tareas:

- Realización de una guía del buen uso de los activos de información.
- Inventariado de los activos de información.
- Clasificación de Activos según MAGERIT, para agilizar el proceso de análisis de riesgos.

Beneficios:

- Conocimiento de la importancia que tienen los activos de información y su adecuada protección.

Responsable: Área de TI

Dominio ISO relacionado	**7.1 Responsabilidad sobre los activo**
Activos del AARR afectados	**El conjunto de todos los activos de la organización**
Amenazas Afrontadas	**Intencionales, No intencionales, Naturales, Industrial**
Tiempo estimado	**6 Meses – Mediano Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 800.00**

ID:	**DOC - 05**
Nombre Propuesta:	**Plan de Recuperación de Desastres (DRP)**
Tipo:	**Documentación**

Detalles

Descripción del proyecto a realizar:

Es necesario tener un plan para saber actuar ante algún evento en relación a desastres naturales, y estar prevenidos, dicho documento está ligado con D0C - 02.

Como todo plan debe tener una debida revisión

Salvaguardas y/o controles principales:

- Planificación de la seguridad
- Inspecciones de seguridad
- Defensa en profundidad
- Climatización
- Formación y Concientización

Tareas:

- Desarrollar un plan de recuperación de desastres naturales (DRP)
- Seguimiento continuo.

Beneficios:

- Estar prevenidos y saber actuar ante alguna eventualidad.
- Conocimiento de los riesgos a los que están expuestos los activos de información.

Responsable: Área de TI

Dominio ISO relacionado	**14.1 Aspectos de la gestión de continuidad de negocio**
Activos del AARR afectados	**El conjunto de todos los activos de la organización**
Amenazas Afrontadas	**Naturales**
Tiempo estimado	**6 Meses – Mediano Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 1, 800.00**

ID:	**PREV - 01**
Nombre Propuesta:	**Gestión de los Backup de los sistemas**
Tipo:	**Prevención**

Detalles

Descripción del proyecto a realizar:

Es necesario estar prevenidos ante ciertos incidentes que puedan darse, por ende, para la protección de la perdida de información, es importante gestionar copias de seguridad de los sistemas, ya que la mayoría de la información se encuentra en este tipo de activos.

Es necesario el uso de buenas prácticas para llevar una buena gestión en este punto. No obstante, una guía puede ser de gran ayuda para la realización de dicha actividad, incluyendo en ella los tiempos y periodos cuando se deba realizar, asimismo el lugar donde se van almacenar.

El responsable de realizar dicha operación, deberá revisar constantemente su actividad y verificar que todo este correcto.

Salvaguardas y/o controles principales:

- Copias de seguridad de los datos (Backup).
- Herramienta de Backup.

Tareas:

- Realizar los procedimientos necesarios para la gestión de Backup.

Beneficios:

- Prevención en la pérdida de información de los sistemas de información
- Conocimiento de los distintos procedimientos a seguir para proteger la información en relación a copias de seguridad.

Responsable: Área de TI

Dominio ISO relacionado	**10.5 Copias de seguridad**
Activos del AARR afectados	**Datos/ información**
Amenazas Afrontadas	**Intencionales, No intencionales, Naturales, Industrial**
Tiempo estimado	**2 Meses – Corto Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 1, 500.00**

ID:	**CONT - 01**
Nombre Propuesta:	**Gestión de acceso al CPD (Informática)**
Tipo:	**Control**

Detalles

Descripción del proyecto a realizar:

Es importante llevar el control de quienes son las personas que tienen accesos a áreas restringidas en este caso al centro de procesamiento de datos ya que es un área muy susceptible, donde se puede perder información valiosa para la organización, por ende controlar los accesos de los empleados es necesario.

En la organización no existen las medidas necesarias para proteger a los activos de información que se encuentran en esta área, por tal motivo es fundamental instalar las medidas necesarias para protegerlos, bien instalando un control físico que ofrezca las ventajas de saber quien accedió y que personas lo intentaron reiteradas veces sin logro alguno.

Salvaguardas y/o controles principales:

- Control de accesos físicos.
- Sistema Biométrico

Tareas:

- Instalación de un sistema para el control de accesos (permitidos y no permitidos).
- Realizar reportes diarios de accesos, para así llevar el control necesario.

Beneficios:

- Reducción de distintas amenazas como robo, pérdidas o fugas de información.
- Incremento en la protección de accesos físicos.
- Conocer que personas intentaron acceder sin éxito alguno.
- Permitir acceso solo a las personas autorizadas.

Responsable: Área de TI

Dominio ISO relacionado	**9.1 Áreas seguras**
Activos del AARR afectados	**Datos/ información/ Instalaciones**
Amenazas Afrontadas	**Intencionales, No intencionales**
Tiempo estimado	**6 Meses – Mediano Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
	Dispositivos físicos.
	Control de accesos.
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 2, 500.00**

ID:	**CONT - 02**
Nombre Propuesta:	**Gestión de roles, responsabilidades y accesos**
Tipo:	**Control**

Detalles

Descripción del proyecto a realizar:

Es necesario conocer los distintos roles que tienen los empleados de la organización, para poder generarle los accesos correspondientes a los sistemas de información, a si pues los involucrados también conozcan cuáles son sus responsabilidades y los accesos a los que están permitidos.

Es importante su revisión continua, para actualizar los permisos, cuando existan cambios.

Salvaguardas y/o controles principales:

- Control de accesos físicos.
- Segregación de tareas.

Tareas:

- Estructurar los roles correspondientes a los diferentes empleados.

Beneficios:

- Disminución de riesgos, teniendo controlados los privilegios del personal.

Responsable: Área de TI

Dominio ISO relacionado	**6.1 Organización interna** **11.1 Requisitos de negocio para el control de acceso** **11.2 Gestión de accesos de usuario** **11.6 Control de acceso a las aplicaciones y a la información** **13 Gestión de incidentes**
Activos del AARR afectados	**Servicios, Aplicaciones, Software, Servidores, personal y Datos.**
Amenazas Afrontadas	**Intencionales, No intencionales**
Tiempo estimado	**4 Meses – Corto Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 1, 800.00**

ID:	**PROC - 01**
Nombre Propuesta:	**Programación segura**
Tipo:	**Procedimiento.**

Detalles

Descripción del proyecto a realizar:

Como se ha visto existen errores de programación, los mismos que pueden ser minimizados si existe un procedimiento de programación segura, evitando los errores que se dan y que se manifiestan cando ya el código se encuentra a disposición de los usuarios.

Uno de los problemas más grandes es que intrusos aprovechen distintas debilidades para acceder a información valiosa, por tanto las revisiones a la red deben ser generadas periódicamente para estar alertas de algún acceso indebido.

Salvaguardas y/o controles principales:

- Gestión de cambios (mejoras y sustituciones)

Tareas:

- Desarrollo de un procedimiento formalizado sobre el ciclo de desarrollo del software (Fase de Pre-Producción).

Beneficios:

- Minimización de los riesgos, y la probabilidad de ocurrencia.
- Procedimientos establecidos y bien definidos para una programación segura.

Responsable: Área de TI

Dominio ISO relacionado	**12.4 Seguridad de los ficheros del sistema** **12.5 Seguridad en los procesos de desarrollo y soporte**
Activos del AARR afectados	**Servicios, Datos y Aplicaciones**
Amenazas Afrontadas	**Intencionales, No intencionales**
Tiempo estimado	**3 Meses – Corto Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 1, 000.00**

ID:	**PROC - 02**
Nombre Propuesta:	**Pruebas del Software**
Tipo:	**Procedimiento.**

Detalles

Descripción del proyecto a realizar:

Este procedimiento va ligado al procedimiento PROC - 01, es una secuencia de pruebas lógicas donde se definirán las pruebas necesarias para controlar los posibles errores por los sistemas de información, mucho antes de que sean puestos en marcha.

Este procedimiento deberá definir quiénes serán las personas con acceso a elaborar dichas pruebas, y también realizar revisiones continuas.

Salvaguardas y/o controles principales:

- Gestión de cambios (mejoras y sustituciones).
- Gestión de vulnerabilidades.
- Cifrado de la información.

Tareas:

- Desarrollar procedimientos para pruebas de software.
- Desarrollo de un procedimiento formalizado sobre el ciclo de desarrollo del software (Fase de pruebas).

Beneficios:

- Minimización de los riesgos, y la probabilidad de ocurrencia.
- Procedimientos establecidos y bien definidos para pruebas de software.

Responsable: Área de TI

Dominio ISO relacionado	**12.2 Tratamiento correcto de las aplicaciones** **12.4 Seguridad de los ficheros del sistema** **12.5 Seguridad en los procesos de desarrollo y soporte**
Activos del AARR afectados	**Servicios, Datos y Aplicaciones**
Amenazas Afrontadas	**Intencionales, No intencionales**
Tiempo estimado	**2 Meses – Corto Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 800.00**

ID:	**PROC - 03**
Nombre Propuesta:	**Cumplimiento de normas y requisitos legales**
Tipo:	**Procedimiento.**

Detalles

Descripción del proyecto a realizar:

Es importante contar con procedimientos estandarizados donde se especifiquen y definan diferentes normativas que el personal que labora en la organización conozca y las apliquen. S e han de tomar en cuenta temas como:

- Manejo adecuado de los activos de información.
- Sanciones, en caso existan por incumplimiento de diferentes normas en relación a seguridad. (Ley de datos personales – superan los 50 UIT)
- Revisiones de auditorías si en caso hubiese, para evaluar las distintas políticas de seguridad implantadas.

Los mismos deben ser revisados cada cierto tiempo (establecido), para nuevas actualizaciones y correcciones, No obstante, dichos procedimientos deben estar al alcance del personal de la organización para su conocimiento.

Salvaguardas y/o controles principales:

- Gestión de cambios (mejoras y sustituciones).
- Gestión de vulnerabilidades.
- Formación y Concientización

Tareas:

- Realizar auto - evaluaciones ligadas a las normas legales existentes.
- Realizar procedimientos referentes a las normas legales.
- Formación de normas legales.

Beneficios:

- Minimización de los riesgos, y la probabilidad de ocurrencia.
- Procedimientos establecidos y bien definidos para pruebas de software.

Responsable: Área de TI

Dominio ISO relacionado	**15.1 Cumplimiento de los requisitos legales** **15.2 Cumplimiento de las políticas y normas de seguridad**
Activos del AARR afectados	**El conjunto de todos los activos de la organización**
Amenazas Afrontadas	**Intencionales, No intencionales**
Tiempo estimado	**3 Meses – Corto Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 1,000.00**

ID:	**PROC - 04**
Nombre Propuesta:	**Auditorías de seguridad**
Tipo:	**Procedimiento.**

Detalles

Descripción del proyecto a realizar:

La entidad debe realizar auditorías de seguridad técnicas, para evaluar las distintas vulnerabilidades a las que esta expuestos sus sistemas y activos de información. Deben ser llevadas a cabo cada cierto tiempo, y realizado por el personal mismo de la organización, para no exponerla a riesgos futuros, dando a conocer las deficiencias existentes.

La entidad debe plasmar distintos procedimientos que den a conocer el estado actual de la organización, especificando cuáles son sus amenazas y vulnerabilidades.

Salvaguardas y/o controles principales:

- Gestión de cambios (mejoras y sustituciones).
- Gestión de vulnerabilidades.
- Formación y Concientización

Tareas:

- Realizar procedimientos referentes a la seguridad de la información, aplicando distintas auditorias y que estén relacionados con la ISO 27001 que involucra el desarrollo de un SGSI.

Beneficios:

- Minimización de los riesgos,
- Procedimientos establecidos y bien definidos para auditorias de seguridad de la información.

Responsable: Área de TI

Dominio ISO relacionado	**12.6 Gestión de la vulnerabilidad técnica** **15.3 Consideraciones sobre las auditorías de SI**
Activos del AARR afectados	**Servicios, aplicaciones, software y datos**
Amenazas Afrontadas	**Intencionales, No intencionales**
Tiempo estimado	**1 Mes – Corto Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 2, 800.00**

ID:	**IMP - 01**
Nombre Propuesta:	**Sistema de detección de intrusos**
Tipo:	**Implantación.**

Detalles

Descripción del proyecto a realizar:

Es importante contar con dispositivos, para la detección de intrusos a los sistemas de información, teniendo acceso a información importante poniendo en riesgo los pilares de la información.

Es necesario evaluar en un determinado tiempo, las distintas actividades realizadas a través de la red.

Salvaguardas y/o controles principales:

- IDS/IPS: Herramienta de detección / prevención de intrusión
- Gestión de vulnerabilidades
- Herramienta para análisis de logs

Tareas:

- Instalación de Sistema de detección de intrusos.
- Asignar responsable para la verificación

Beneficios:

- Minimizar y prevenir ataques futuros.
- Seguridad en el manejo de la información.

Responsable: Área de TI

Dominio ISO relacionado	**10.6 Gestión de la seguridad de las redes**
Activos del AARR afectados	**Servicios y aplicaciones**
Amenazas Afrontadas	**Intencionales, No intencionales**
Tiempo estimado	**1 Mes – Corto Plazo**

Estimación de Coste

Presupuesto del costo económico.

Recurso:	**Horas laborables por el personal a cargo del proyecto.**
Dedicación:	**Constante - Responsables**
Coste Total:	**S/. 1, 000.00**

PS 1.- Plan de ejecución

PS1.1 Planificación de los proyectos

En este apartado se dará a conocer la duración y el valor económico de los proyectos seleccionados, los mismo que han sido organizados según la prioridad de la organización en base a las salvaguardas a las que atribuye y que se necesitan para mitigar o reducir los riesgos de nivel muy alto y alto. (Ver Anexo N°17)

1er año (2016):

- Política de seguridad.
- Gestión de los Backup de los sistemas
- Gestión de roles y accesos
- Implantación Sistema de detección de intrusos

2do año (2017):

- Gestión de acceso al CPD
- Procedimiento de cumplimiento de normas y requisitos legales
- Documento del plan de continuidad de negocio (BCP)
- Documento del plan de Recuperación de Desastres (DRP)
- Procedimiento de programación segura
- Procedimiento de pruebas del software
- Documento mantenimiento de sistemas
- Listado de activos
- Auditorías de seguridad

La razón de escoger estos proyectos en ese orden se debe que dentro del análisis de riesgos se observaron las deficiencias de la organización de no contar en una primera instancia con políticas de seguridad, cuyos objetivos, permiten poder de una u otra forma salvaguardar los activos de información de los riesgos, ahora bien, la gestión de Backup de los sistemas, se deben a las deficiencias de las datos al no contar con copias de seguridad y si existen se encuentran con un eficacia escasa. En cuando a la gestión de roles y accesos, debido a que la mayoría de las amenazas identificadas que son las que más se pueden efectuar son las de tipo errores y fallos no intencionales (43%), así mismo la instalación de IDS para combatir con los ataques intencionados que abarcan el 33% de

amenazas en la organización. Algunos de los proyectos se podrán realizar de forma paralela (Ver Anexo N°01)

A continuación se muestra un detalle de los proyectos por tiempo de implementación (Meses).

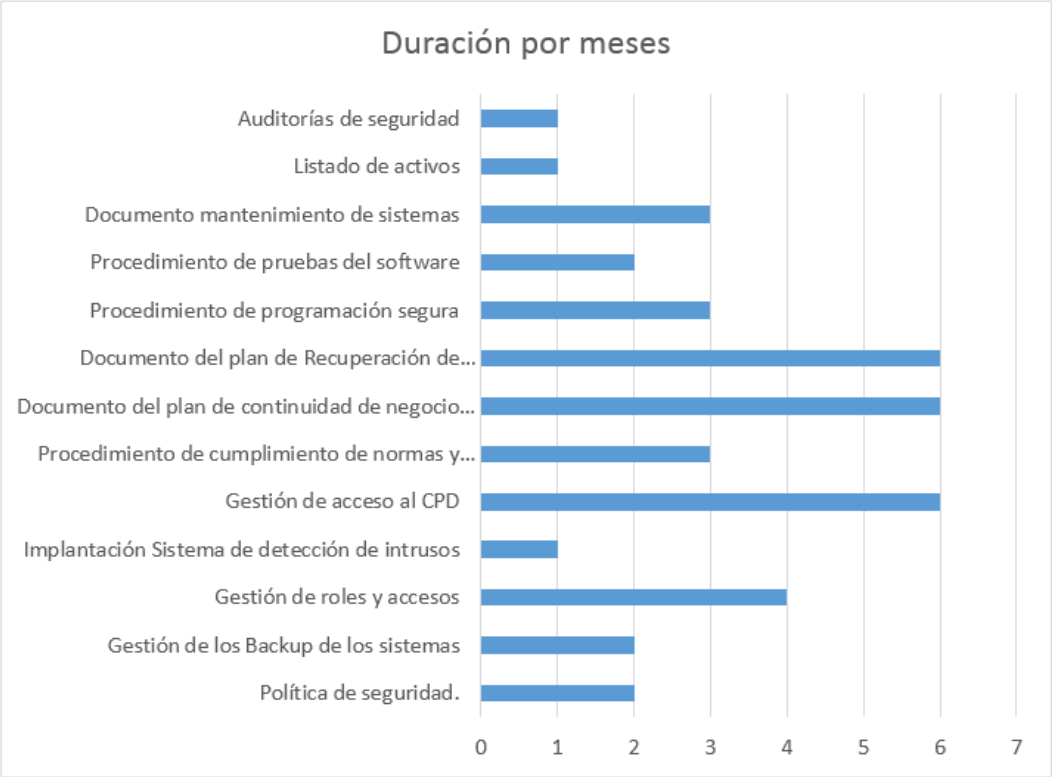


Grafico N°01: Proyectos por tiempo de implementación

PS2.1 Planificación económica

Se distribuyó los costos de inversión de forma anual para obtener el presupuesto total. Dichos valores son una aproximación de los costos que implicaría la ejecución de los proyectos, teniendo en cuenta que el personal del área de TI, labora dentro de la organización.

1er año (2016)	S/. 4,800.00
2do año (2017)	S/.12,900.00
Total	S/. 17,700.00

A continuación se muestra un detalle de los proyectos por costo de implementación.

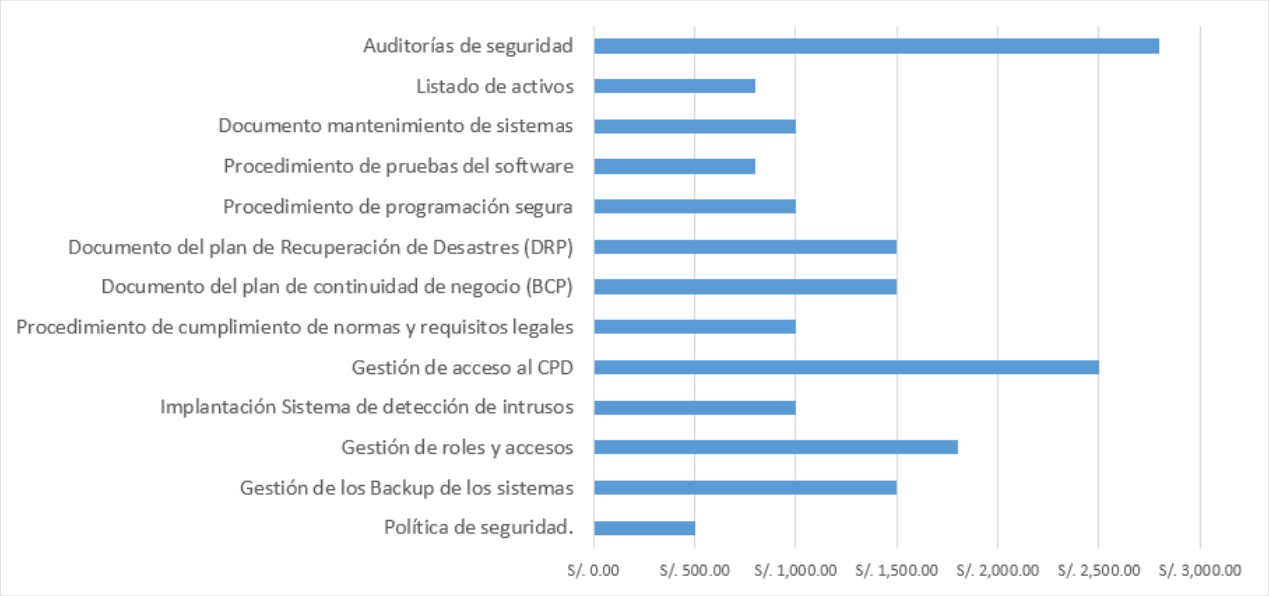
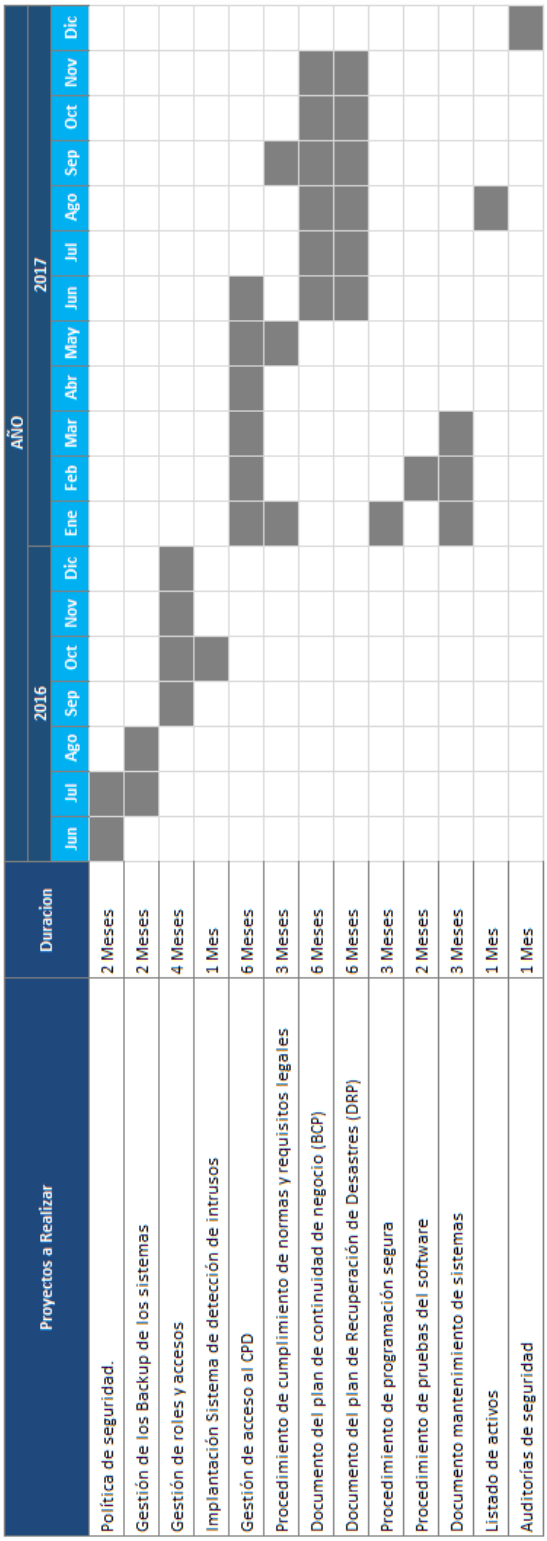


Grafico N°02: Proyectos por costo de implementación

Anexos N°01: Diagrama Temporal de los proyectos a realizar.



Anexos N°02: Cuadro de Costos

1er año (2016)	
Política de seguridad.	S/. 500.00
Gestión de los Backup de los sistemas	S/. 1,500.00
Gestión de roles y accesos	S/. 1,800.00
Implantación Sistema de detección de intrusos	S/. 1,000.00
Total Anual (2015)	**S/. 4,800.00**
2do año (2017)	
Gestión de acceso al CPD	S/. 2,500.00
Procedimiento de cumplimiento de normas y requisitos legales	S/. 1,000.00
Documento del plan de continuidad de negocio (BCP)	S/. 1,500.00
Documento del plan de Recuperación de Desastres (DRP)	S/. 1,500.00
Procedimiento de programación segura	S/. 1,000.00
Procedimiento de pruebas del software	S/. 800.00
Documento mantenimiento de sistemas	S/. 1,000.00
Listado de activos	S/. 800.00
Auditorías de seguridad	S/. 2,800.00
Total Anual (2015)	**S/. 12,900.00**
Total de proyectos de seguridad	**S/. 17,700.00**

Anexo N°18 Manual De Políticas Y Estándares De Seguridad Informática

---

CLINICA INTERNACIONAL – PIURA

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA DE CLÍNICA INTERNACIONAL

Manual de Políticas y Estándares (MPE)

Propósito

La finalidad de este documento es la de describir las diferentes políticas y estándares de seguridad que los usuarios tanto de las áreas de tecnología como colaboradores de la organización deberán considerar para proteger los activos de información que posee Clínica Internacional Piura minimizando los diferentes riesgos a los que se encuentran expuestos.

Introducción

Todo organización tiene como fin brindar un servicio de calidad y a la vez mantener sus funciones adecuadamente cuando una organización se encuentra en riesgo puede ocasionar que la continuidad de su negocio se ponga en peligro Asimismo su funcionamiento será ineficiente e ineficaz por ello la definición de políticas y estándares adecuados para la seguridad de la información es un punto principal que se debe tomar en cuenta.

La seguridad de la información se encarga de proteger a los activos de información en este caso basándose en políticas y estándares qué Clínica Internacional sede Piura requiere y necesita.

Cabe mencionar que existe un estándar denominado hizo ISO/IEC 27002: 2013 que viene a ser un conjunto de buenas prácticas que brindan seguridad de la información a una organización la misma que consta de dominios de control y objetivos de control los cuales pueden ser adaptado y aplicados de acuerdo a la organización.

Objetivo

Minimizar los riesgos encontrados en la organización estableciendo y difundiendo las políticas y estándares de seguridad de la información a todos los colaboradores que

pertenecen a dicha entidad, para su conocimiento y su debido cumplimiento.

Alcance Este documento contiene las políticas y estándares de seguridad de la información que deben cumplir todos los colaboradores de la organización para mantener la continuidad del negocio.

Justificación Se realizó un previo análisis permitiendo conocer el estado actual de la organización lo mismo que permitió definir las políticas y estándares para la seguridad de los activos de información.

Beneficios Dichas políticas y estándares de seguridad de la información definida en este manual son base fundamental para proteger a los activos de información que se encuentran en riesgo dentro de la organización

Sanciones por incumplimiento El incumplimiento de las políticas plasmadas en este documento, debe ser de estricto cumplimiento, ya que si no es el caso, se darán sanciones por irresponsabilidades administrativas, siendo estas aplicadas por el personal autorizado.

1. POLÍTICAS DE SEGURIDAD

Política	Las áreas de la organización deben tener un manual de procedimientos que indique detalladamente las actividades que se realizan, asimismo el manual de políticas de seguridad correspondiente.
Conjunto de políticas para la seguridad de la información.	El área de informática será el encargado de distribuir el manual de procedimientos y estándares de seguridad de la información a los diferentes usuarios de los medios tecnológicos pertenecientes a la organización.
Revisión de las políticas para la seguridad de la información	Las políticas plasmadas en el manual de políticas y estándares tendrán una revisión bimestral para su óptimo funcionamiento y su actualización.

2. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Política	El personal tanto interno como externo que pertenezca a la organización, sea personal nuevo o antiguo deberá respetar los acuerdos de confidencialidad de seguridad de la información y uso correcto de los diferentes recursos de información, así como adecuarse y adoptar las políticas de seguridad de la información plasmada en el manual de estándares y política.
Obligaciones De los Usuarios	Como parte de la contratación de personal, se deberá agregar un documento de compromiso de confidencialidad o no divulgación de información, el mismo que será firmado por el personal contratado, donde el mismo acepta las responsabilidades y las sanciones correspondientes al incumplimiento de lo estipulado en el documento mencionado.

Dicho documento firmado, será recepcionado y almacenado por el personal de recursos humanos, el mismo que será estudiado cuando exista algún tipo de incumplimiento por parte del personal.

El personal contratado debe haber leído detenidamente lo estipulado en dicho documento, para que no queden dudas de lo que debe y no debe hacer.

Instrucción de personal

Todo usuario de activos informáticos recibirá una adecuada capacitación y actualización periódica en materia de seguridad de información.

El personal de TI será la persona encargada de instruir al personal para que tenga conocimiento del manual de políticas y estándares, donde se podrá conocer las obligaciones y medidas en caso de la indisciplina de éste.

Medidas disciplinarias

El personal de TI deberá verificar que se cumplan los acuerdos de confidencialidad, por parte del personal contratado.

Sanciones

Es considerada una infracción cuando usuarios de servicios de tecnologías de información, incumplen el acuerdo de confidencialidad firmado.

3. GESTIÓN DE ACTIVOS

Política	El personal de TI se encargará de la realización del inventario de todos los activos de la organización así como el resguardo y recepción de la firma del usuario como responsable del activo que se le asigne y de conservarlo en la ubicación actual.
Inventario de Activos	El personal de TI deberá identificar cuáles son los activos más importantes según su sensibilidad y criticidad de la organización, identificando a la vez los usuarios, la ubicación, y otros datos que sean necesarios para la elaboración del inventario de activos. El personal encargado de la elaboración del inventario deberá tenerlo actualizado en caso de alguna modificación, como también tendrá la obligación del revisado y evaluación del mismo, con una periocidad no mayor a 4 meses. El encargado del inventariado tendrá la obligación de clasificar los activos físicos de la organización y realizar el etiquetado conveniente.
Mantenimiento de activos.	El área de TI deberá establecer un cronograma de mantenimiento de activos físicos para su óptimo funcionamiento del mismo
Obligaciones del personal	Todo usuario de equipos informáticos se hará responsable del activo físico que se le designe firmando un documento de responsabilidad de activos. Asimismo, deberá avisar inmediatamente si se diera el caso de la pérdida de algún activo que este bajo su jurisdicción.

4. CONTROLES DE ACCESO

Política

El personal de TI es el encargado de los accesos que son proporcionados a los colaboradores de la organización, como accesos a los sistemas información o al centro de procesamiento de datos de Clínica Internacional – Sede Piura, es el personal encargado de realizar el proceso conveniente para verificar y asignar los diferentes accesos a la información.

Administración de accesos

El personal a cargo de la seguridad de la información, deberá definir el procedimiento necesario para el registro de usuario, controlando de esta manera, cuando se brinde o anule algún tipo de acceso bien a bases de datos, servicios de información, acceso a red, etc. limitando y controlando la asignación y uso de privilegios.

Sólo personal de TI podrá realizar configuraciones, instalaciones de aplicaciones, accesos de dispositivos físicos, etc., que ponen en riesgo la integridad, disponibilidad y confidencialidad de la información, protegiéndolas mediante contraseñas o bloqueos necesarios.

El personal de TI, tendrá la obligación de deshabilitar los puertos USB. Disquetera, etc. que puedan permitir la fuga de información mediante, herramientas de almacenamiento externo.

El personal de TI, tendrá la obligación de restringir páginas web de redes sociales, que interrumpen las labores del personal, así mismo evitar permisos de

instalación y/o desinstalación de programas de los equipos informáticos.

Responsabilidades De Usuarios

A cada usuario se le asigna un usuario y una contraseña, por tanto el mismo será el responsable de protegerlas y no compartirlas con nadie, ya que con esa información accederán a los recursos asignados al usuario.

Es Responsabilidad de los usuarios autentificarse en los controles de accesos que la organización posea, para que puedan acceder a la infraestructura tecnológica.

El personal no debe compartir información crítica referente a los accesos de la infraestructura tecnológica, sin primero estar autorizado por el personal correspondiente.

Está prohibido que los usuarios compartan el usuario y contraseña asignada, ya que si se viola alguna regla, atentando con los pilares de la información, se sancionará al usuario que realizó diferentes actividades a menos que se comprueba que se usurpo el usuario.

Los usuarios deberán mantener sus equipos de trabajo, con medidas de bloqueo evitando el acceso de cualquier persona cuando se aíslen o ausenten de su Workstation (estación de trabajo).

Administración De privilegios

Cualquier modificación de roles y responsabilidades asignándoles nuevos privilegios de acceso al personal, será comunicado al área de TI, el mismo que enviará el formato de modificación de accesos, para que sea completado adicionalmente, de contener la firma del jefe

	responsable de la asignación de accesos, para que el área pueda, realizar los ajustes necesario.
Administración Y uso de contraseñas	Los usuarios y contraseñas asignadas son únicas, por tal motivo, está prohibido el uso de contraseñas compartidas. Cuando un usuario olvide su contraseña, deberá reportarlo al área de TI especificando que tipo de acceso es y el motivo de su solicitud, para que el área de TI proporcione una nueva contraseña. La obtención o cambio de una contraseña debe hacerse de manera formal; reportando al área de TI, el mismo que confirmará la identidad del usuario. Está prohibido que la asignación de usuario y contraseña estén plasmada en medios físicos o impresos para que sean visibles para que personas no autorizadas tengas acceso. Todo usuario que sospeche de que su usuario ya no es privado, deberá cambiarlo inmediatamente, para evitar futuros riesgos. El Jefe de Sistemas, o la persona que el designe, tendrá la responsabilidad de actualizar los perfiles de usuarios asignados.
Accesos Remotos	Quedan totalmente prohibido las conexiones a redes externas, con cualquiera que sea el medio de comunicación. Si alguna persona que por algún motivo

se le otorgue ese beneficio, tendrá que ser documentada y tener previa autorización de la dirección.

No está permitida la administración remota, si no se cuenta con la autorización y la seguridad necesaria autorizada por la Dirección.

5. SEGURIDAD FÍSICA Y AMBIENTAL

Política	Solo personal autorizado podrá, ejercer diferentes funciones como la reubicación, mantenimiento de los equipos informáticos, como la seguridad óptima de estos activos, permitiendo los accesos necesarios.
Resguardo y protección de la información	El usuario tiene la obligación de resguardar los dispositivos de almacenamiento auxiliares que estén bajo su responsabilidad Si se ingresan equipos que no sean pertenencia de CI – Sede Piura, y la duración de su estadía en las instalaciones de la misma es mayor a un día, se deberá realizar el procedimiento indicado, es decir que la persona responsable del activo deberá firmar la autorización de salida.
Protección y ubicación de los equipos	Está prohibido reubicar los equipos de trabajo, así como la instalación de diferentes dispositivos, entre otros activos sin autorización de las personas responsables. Si se necesita realizar alguna de estas actividades será necesario solicitar los servicios necesarios. Las unidades de trabajo (equipos informáticos), serán solo para uso exclusivo de las funciones encomendadas al personal.

La capacitación de los usuarios por manejo de las herramientas de trabajo, es su responsabilidad, el mismo que deberá tenerlo como requerimiento para que el área de TI pueda realizar dicha capacitación evitando futuros riesgos.

El almacenamiento de la información crítica para los usuarios debe realizarse en las unidades asignadas por el área de TI.

La ingesta de alimentos y bebidas en las estaciones de trabajo están prohibidas, ya que los equipo de cómputo, deben encontrarse en un lugar adecuado y cuidado.

El personal de TI, deberá encargarse que los cables de conexión estén ubicados adecuadamente previniendo que éstos sean pisados o que se puedan colocar objetos encima de ellos.

Únicamente Personal autorizado podrá realizar algún cambio o reubicación de algún equipo informático previo anuncio.

Mantenimiento De equipos

Solo personal autorizado podrá darles mantenimiento a los equipos, ese es el personal encargado de abrir o destapar los equipos de cómputo.

Los usuarios tienen la obligación de seleccionar y crear copias de seguridad a la información crítica cuando los equipos sean llevados a mantenimiento evitando la perdida involuntaria.

El personal de TI realizará un mantenimiento preventivo periódicamente. (Bimestral o trimestral), dependiendo de la entidad.

6. SEGURIDAD EN LA OPERATIVA

Política	Todo personal que requiera un servicio con relación a tecnología debería contactarse con el responsable del área de TI para establecer los procedimientos necesarios para la realización de la solicitud.
Procedimientos De operación	Se deberán documentar los distintos procedimientos operativos además su actualización está a cargo del responsable de TI.
Instalación de Software	Los usuarios que requieran la instalación de software, deberán justificar su utilización hacia su jefatura la misma solicita al área de TI el documento necesario para el requerimiento, el mismo que se realizara siempre y cuando este la autorización (firma y sello) de la jefatura correspondiente. Una de las faltas graves que serán sancionadas es la instalación de softwares sin llevar a cabo el procedimiento adecuado. El encargado de TI, deberá instalar herramienta de actualizaciones, a las pc de la organización, que cuenten con el resguardo de la información.

Identificación del incidente	Cuando exista el conocimiento o desconfianza de que se atentado contra el pilar de integridad de la información de los distintos organismos administrativos, el usuario informático deberá informar al titular. El personal de TI tendrá una bitácora donde se registrará los problemas encontrados y las soluciones, brindadas a dicho problemas.
Seguridad de la red	Se considerará un ataque por parte de los usuarios de las tecnologías de información aquellas actividades que tienen fines de encontrar las vulnerabilidades del sistema.
Uso del correo electrónico	La información trasmitida vía correo electrónico interno deberá ser considerada como información crítica y propiedad de Clínica Internacional. Los mensajes deben ser manejados tomando en cuenta los pilares de la información. Ser confidenciales, estar disponibles entre receptor y emisor e íntegros. El uso del correo institucional será utilizado para la realización de actividades internas asignadas a los distintos usuarios que laboran dentro de la organización, alguna difusión de mensajes emitidos serán sancionados. Queda completamente prohibido alterar la información emitida por el correo institucional.
Controles contra código malicioso	Para salvaguardar los activos de información el usuario no debe instalar software que no esté autorizado por el área de TI. Si se usan equipos auxiliares como memorias USB, discos, etc. los usuarios deberán estar seguros de que no estén

infectados, ejecutando el antivirus que proporciona el área de TI.

Si hay sospechas de que algún virus se está ejecutando, el usuario deberá informar de inmediato al área de TI, para evitar riesgos.

Uso de Internet

Los usuarios deberán utilizar el internet solo para uso exclusivo de las necesidades para operar sus funciones.

La accesibilidad al internet deberá ser provista por el área de TI, así mismo si es necesario que algún usuario requiera de este servicio, deberá justificarlos a su jefatura correspondiente, la misma que solicitará el acceso al área de TI, mediante un documento, cuyo documento será firmado y autorizado por su jefatura.

Si a los usuarios se les presenta algún incidente, deberán comunicarlo de inmediato al área de TI

Los usuarios que tienen acceso a al servicio de internet aceptan que:

- Estarán monitoreado sus actividades por este servicio.
- No ingresaran a páginas que no sean de utilidad de la organización.
- Serán sancionados si emiten información confidencial de la organización.
- Está prohibida la descarga de archivos que no sean solicitados por la dirección.
- El uso del internet es exclusivo para actividades de la organización.

7. GESTION DE INCIDENCIAS SI

Política	El área de informática será el responsable de la realización de una bitácora donde se registrarán los incidentes ocurridos en el transcurso del tiempo, dándoles una valoración por evento, así como también tener actualizado el análisis de riesgo que la Clínica Internacional – Sede Piura pueda estar expuesta.
Realización de Bitácora	El personal de Informática será el encargado de registrar cada evento ocurrido dentro de la organización, que soluciones se le dio a ese suceso. Que personal participó, cuando ocurrió y que nivel de gravedad tuvo. Cada empleado que labore dentro de la organización y haga uso de activos tecnológicos deberá informar al área de Informática los problemas que ocurren en el día y que impiden realizar sus labores.
Periodo de evaluación	El área de Informática será encargada de realizar periódicamente la valoración de riesgo de los sucesos ocurridos en la Clínica Internacional, valiéndose de la bitácora donde se encuentra el registro de sucesos diarios.

Aprendizaje	El personal nuevo deberá informarse de los sucesos ocurridos, de las incidencias para poder brindar una respuesta cada vez que pueda ocurrir un suceso parecido.

8. CUMPLIMIENTO

Política	El manual de estándares y políticas deberá ser observado y controlado por el personal de informática quien realizara, periódicamente un control de cumplimiento de los controles establecidos, para poder garantizar acciones preventivas y correctivas de los servicios de TI.
Cláusulas de cumplimiento	Las políticas serán evaluadas periódicamente y modificadas dependiendo de un consenso con la dirección para así también poder implementar mecanismos de control. Las jefaturas deben apoyar al área de TI con verificar el cumplimiento de las políticas y estándares establecidos en el manual de usuarios.
Violaciones de Seguridad Informática	Está prohibido el uso de herramientas que quebranten las salvaguardas o controles establecidos, así mismo la realización de fallas del sistema de seguridad, sólo está permitido siempre y cuando sea por motivos necesarios y con autorización de los responsables correspondientes. Ningún empleado y/o usuario podrá atentar con los activos de información, introduciendo algún código malicioso (virus, troyano, etc.) con la finalidad de afectar el desempeño de los mismos y sacar beneficio propio.