UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"Análisis y valoración de riesgo de la infraestructura tecnológica en el segundo local del Gobierno Regional Piura usando la metodología Magerit"

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Delgado Mena, Javier Eduardo (ORCID: 0000-0001-5474-664X)

ASESOR:

Mg. Quito Rodríguez, Carmen Zulema (ORCID: 0000-0002-4340-5732)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

PIURA – PERÚ

2019

DEDICATORIA

A Rolando mi hermano porque compartiste conmigo momentos que nunca voy a olvidar y ahora que estas en el cielo te pido ilumines mi camino en los momentos más difíciles.

Gracias por apoyarme, por consentirme y por todo el afecto de cariño que me mostraste, te quiero hermano y siempre te voy a llevar en el corazón.

AGRADECIMIENTO

Un millón de gracias a todos mis docentes por haber contribuido en mi formación profesional, por servirme de ejemplo y ganas de superación.

A mi familia que siempre están para mí y me apoyan en las buenas y malas.

A mis amigos que son el reflejo de lo que soy y lo que pretendo ser.

Al Ingeniero Víctor Manuel Mena Gutiérrez por aceptar el desarrollo del presente estudio en el Gobierno Regional Piura, a los Ingenieros Henry Nunura, Manuel Ramírez y Walter Odicio por brindar la información necesaria para el óptimo desarrollo de las distintas fases de la metodología.

Índice de contenidos

Resumen

Un análisis de riesgo consiste en identificar los peligros que afectan a la seguridad de la información, determinar su magnitud y determinar las áreas que necesitan salvaguardas. No todos los activos tecnológicos son vulnerables a las mismas amenazas, es por ello que se opta por realizar un análisis de riesgo para determinar la probabilidad de la materialización de una amenaza sobre un activo, las cuales pueden manifestarse de dos formas, intencionales o accidentales.

Para llevar a cabo esta investigación se hizo uso de la metodología española MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas) la cual establece una serie de pasos para desarrollar fase a fase el análisis de riesgo.

Se optó por seleccionar una muestra de 348 activos. La selección de ordenadores fue de la siguiente forma, se hizo uso el software Nessus herramienta Nessus v6.4.3 y se escaneo las 130 primeras IP de la subred (172.16.11.1 - 172.16.11.130) y 30 de la subred perteneciente a servidores (172.16.8.1 - 172.16.8.30), dando un total de 160 ordenadores analizados, los otros activos de Comunicación, Soporte de Información, Equipos Auxiliares, etc. se tomaron en su totalidad.

Los instrumentos y técnicas que se utilizaron en la recolección de datos fueron guías de observación (hoja de registro), donde se anotaron los activos de información, las amenazas, el escaneo de vulnerabilidades y salvaguardas.

Entre los principales resultados obtenidos en las distintas fases de la metodología tenemos que el 66% de los activos relevantes se encuentran en un nivel de criticidad de riesgo Muy Alto (nivel 4), debido a que las amenazas evaluadas en las distintas dimensiones de seguridad varían en un nivel de degradación de valor, Alto y Muy Alto por ende su nivel de probabilidad e impacto es mucho mayor. La amenaza con mayor nivel de degradación de valor (Muy Alta) es la de fuego en las capas de equipos y comunicaciones, es decir la posibilidad de que el fuego acabe con los recursos informáticos.

Palabras clave: Análisis de riesgo, Amenazas, Impacto, Riesgo, MAGERIT.

Abstract

A risk analysis is to identify hazards that affect the security of the information, determine its magnitude and identify areas that need safeguards. Not all technology assets are vulnerable to the same threats, that is why we choose to perform a risk analysis to determine the likelihood of the realization of a threat on an asset, which can take two forms, intentional or accidental.

To carry out this research was the use of Spanish MAGERIT methodology (Methodology Risk Analysis and Management of Information Systems of Public Administration) which establishes a series of steps to develop phase-to-phase risk analysis.

It was decided to select a sample of 348 assets. Computer selection was as follows, use is made Nessus software 130 and the first IP subnet (172.16.11.1 - 172.16.11.130) is scanning and 30 belonging to the subnet servers (172.16.8.1 - 172.16. 8.30), giving a total of 160 computers scanned, the other assets of Communication, Information Support, auxiliary equipment, etc. They were taken in full.

The tools and techniques used in data collection were observation guides (recording sheet), where information assets are recorded, the threats, vulnerability scanning and safeguards.

The main results obtained from the various phases of the methodology we have 66% of the relevant assets are at a level of criticality very high risk (level 4), because the threats evaluated in different security dimensions vary at a level of degradation of high and very high hence its level of probability and impact is much greater. The threat with higher value degradation (Very High) is the Fire in layers and communications equipment, that is the possibility that the fire destroys computing resources.

Keywords: Risk Analysis, Threat, Impact, Risk, MAGERIT.

I. INTRODUCCIÓN

Es casi una obligación de los administradores de red tomar medidas más activas y preventivas, con el fin de luchar contra la delincuencia informática. Comprender las vulnerabilidades es fundamental para entender las amenazas que representan y con ello el riesgo potencial en la organización.

Una vulnerabilidad es un conjunto de condiciones que permite la violación explícita o implícita de una política de seguridad, (Aguilera López, 2010). No todos los activos son vulnerables a las mismas amenazas, es por ello que se opta por realizar un análisis de riesgo para determinar la probabilidad de la materialización de una amenaza sobre un activo, las cuales pueden manifestarse de dos formas, intencionales o accidentales. Por lo tanto, llegamos a la conclusión que un ataque es la materialización de una amenaza intencional que aprovecha las vulnerabilidades de un sistema para su efectividad.

En la actualidad muchas de las empresas omiten realizar un análisis de riesgo, algunas veces por cuestiones de tiempo u otras por dinero. Suelen optar sólo por un estudio de vulnerabilidades, las cuales por sí mismas no causan daño, pero sí cuando son explotadas por alguna amenaza.

Para llevar a cabo esta investigación se hizo uso de la metodología española MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas) la cual permitió desarrollar fase a fase el análisis de riesgo, además se hizo uso de técnicas de escaneo del Hacking para la detección de las vulnerabilidades lógicas.

El nivel de seguridad de la información del Gobierno Regional Piura es muy deficiente, si bien es cierto se cuenta con controles de seguridad como un Firewall perimétrico Fortigate, copias de seguridad, active directory, políticas de navegación, de correo, etc. Existen muchas vulnerabilidades físicas, de procesamiento, de mantenimiento preventivo, debilidad en la estructura de contraseñas, ausencia de antivirus o falta de actualización, condiciones inadecuadas de temperatura y humedad, etc.

A simple vista los activos de información más vulnerables son, el usuario que no es capacitado sobre las amenazas informáticas, la importancia de proteger la información, los daños que provocaría el mal uso de los puntos eléctricos (para ello es necesario

capacitar en Seguridad y Salud en el Trabajo); la información, la acción de crear copias de seguridad diarias pero almacenarlas en el mismo local en la misma área y al alcance y vista de todos hace que ese control de seguridad disminuya su eficiencia acarreando la materialización de amenazas que afecten la disponibilidad de toda la información de la organización y los equipos informáticos en especial el Data Center, el cual es amenazado por condiciones inadecuadas de temperatura y humedad, degradación de los soportes de información, destrucción de la información, acceso no autorizado, etc. pues ésta área de comunicaciones no cuenta con aire acondicionado sólo ventiladores, la distribución y ubicación de los equipos no tiene un estándar que garantice su seguridad, no tiene controles perimétricos ni ambientales, es por ello que se presentará una propuesta de implementación de un Data Center que este alineado a los requerimientos mínimos solicitados por la ISO 942, que es un estándar que define la infraestructura de soporte de un Data Center.

En el año 2012, los autores Mejía Londoño y otros, realizan un estudio titulado "Vulnerabilidades, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos de las organizaciones**".**

En dicho estudio, los autores, proporcionan un análisis de los ataques informáticos y su efecto o impacto en los procesos operacionales de la organización, además realizan un análisis de cómo prevenir, detectar y mitigar las vulnerabilidades y amenazas que se materializan en ataques informáticos hacia la red de datos de la organización.

Para los autores el elemento más débil por dónde empezar a atacar es el usuario donde su ingenuidad es la principal debilidad para la ingeniería social, propone como método de prevención aplicar políticas de seguridad y dar a conocer el valor de la información para la organización, además establece que la fase de detección se convierte en el factor más importante ya que desde allí empiezan a disminuir las amenazas de un ataque. Por lo tanto, un constante monitoreo y auditorias nos permiten descubrir las falencias que presenta la organización.

En el año 2013, la autora Gaona Vásquez desarrolla su tesis de grado titulada "Aplicación de la Metodología MAGERIT en el Análisis y Gestión de Riesgos de la Seguridad de la Información aplicado a la Empresa Pesquera e Industrial Bravito S.A en la ciudad de Machala".

El objetivo del estudio es lograr obtener un mayor nivel de seguridad de la información seleccionando controles o salvaguardas proporcionales a los riesgos informáticos presentes y el nivel de importancia del activo de información a proteger. Usa la metodología MAGERIT ya que se ajusta a las necesidades del proyecto, para la recolección de datos se basa en el libro 2 - Catálogo de Elementos MAGERIT v3 y para el procesamiento de los datos tanto para la valoración y estimación de activos, amenazas, impacto, riesgo y salvaguardas hace uso de la herramienta Pilar 5.2.9.

Como resultados obtenidos nos muestra los activos de información que poseen un nivel de riesgo alto, a fin de implementar controles que permitan minimizar el impacto y probabilidad de la materialización de una amenaza.

Concluye que gracias a la metodología se obtuvieron resultados reales del estado actual del nivel de riesgo informático en la empresa seleccionando las salvaguardas o medidas necesarias para mitigar o reducir el nivel de riesgo. Hizo uso de la herramienta Pilar 5.2.9 que le permitió determinar de manera directa los mecanismos o controles de seguridad que fueron necesarios implementar en la empresa.

La adquisición de conocimiento de la autora es la forma de identificación y valoración de los distintos puntos de la metodología usando la herramienta propia de MAGERIT llamada PILAR.

II. MARCO TEÓRICO

Encargarse de la seguridad de la información en una organización no es fácil, existe mucha información sobre vulnerabilidades y ataques en su mayoría son conocidos y están muy bien documentados, en internet usando motores de búsqueda los atacantes pueden encontrar vulnerabilidades de cualquier producto o sistema.

Según Nando (2010) la labor de un profesional responsable de la seguridad de la información va mucho más allá que una simple protección de datos contra virus informáticos, al contrario protege la mayoría de los activos más importante de la organización, desafortunadamente los atacantes pueden encontrase dentro de la red (insiders), El mismo autor menciona la importancia de realizar un análisis de riesgo de seguridad la información, permitiendo tomar acciones preventivas si los resultados muestran que algún activo de información se encuentra en un nivel de riesgo no aceptable por la organización.

Según Nando (2010) este análisis de riesgo consiste en realizar los siguientes pasos, identificar los activos de información, evaluar las vulnerabilidades, identificar las amenazas y estimar el nivel de riesgo informático, permitiendo identificar y valorar los activos de información que necesitan ser protegidos.

Para realizar un análisis de riesgo debemos tener en cuenta lo siguiente (Nando, 2010):

- **Qué necesita proteger:** Debemos identificar y valorar los activos de información determinado su nivel de importancia.
- **De quién debe protegerlo:** Debemos identificar las vulnerabilidades informáticas que pueden ser aprovechadas por las amenazas para materializarse.
- **Cómo protegerlo:** Debemos evaluar contramedidas o salvaguardas que nos permitan mitigar el nivel de impacto de las amenazas y con ello el nivel de riesgo tecnológico.

Un análisis de riesgo según Areitio Bertolín (2008) es un proceso que consiste en identificar los riesgos que afectan la seguridad de la información, permitiendo identificar las áreas que necesitan salvaguardas o controles de protección determinando la magnitud del riesgo, el impacto y probabilidad de ocurrencia de las amenaza. Existen distintas metodologías para realizarla, en este estudio usaremos

MAGERIT una metodología española que permite estimar los riesgos de seguridad de la información a los que está expuesta una organización.

Los objetivos que persigue la metodología son: sensibilizar a los responsables de la información sobre la existencia de riesgos y la necesidad de gestionarlos, ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de las TIC y ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control (Gómez y otros, 2012).

Para realizar la evaluación de riesgo la metodología MAGERIT establece seguir los siguientes procedimientos: identificar los activos de información y definir su criticidad, identificar las amenazas a los cuales están expuestos los activos, identificar los controles de seguridad implementados e identificar su eficacia frente al riesgo, estimar el impacto y probabilidad de ocurrencia de las amenazas, permitiendo estimar el nivel de riesgo (Gómez y otros, 2012).

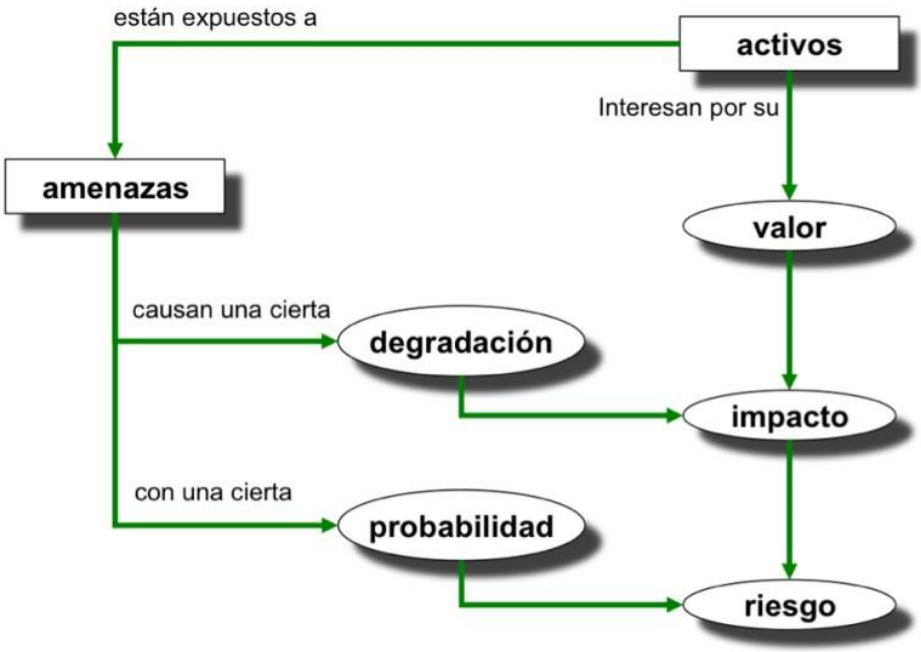


Figura Nº 01 – Estructura del Análisis de Riesgo
Fuente: MAGERIT – versión 3.0

Además, acota 7 informes para la documentación final que son el hallazgo y conclusiones del análisis de riesgo:

Modelo de valor, Según Amutio Gómez, y otros (2012) incluye la descripción de los activos de información, sus dependencias, y estimación de valor en cada dimensión.
Mapa de riesgos, Según Amutio Gómez, y otros (2012) incluye el detalle de las amenazas, la valoración de la frecuencia de ocurrencia y degradación de valor que causaría la materialización de la amenaza.
Declaración de aplicabilidad, Para Amutio Gómez, y otros (2012) debe indicar si las salvaguardas implementadas son eficaces o carecen de sentido.
Evaluación de salvaguardas, Para Amutio Gómez, y otros (2012) incluye la evaluación de la eficacia de los controles existentes en proporción al nivel de riesgo que afrontan.
Informe de insuficiencias o vulnerabilidades, Para Amutio Gómez, y otros (2012) permite identificar y documentar las salvaguardas que son necesarias, pero están ausentes así mismo la evaluación o identificación de vulnerabilidades que podrían ser aprovechadas por las amenazas para materializarse.

Empezando a definir la metodología, como primera fase tenemos la identificación y valoración de activos, toda organización posee activos susceptibles de ser atacados de forma intencional o accidental con consecuencias para la entidad, según Amutio Gómez, y otros (2012) en un sistema de información hay dos cosas esenciales, la información que se maneja y los servicios que se prestan, además existen otros tipos de activos relevantes o capas como los denomina Amutio Gómez, y otros (2012) en la metodología MAGERIT v3: los datos materializan la información; los servicios permiten manejar los datos; los equipos informáticos permiten hospedar datos, aplicaciones y servicios; los soportes de información son dispositivos de almacenamiento de datos; el equipamiento auxiliar complementa el material informático; las redes de comunicación permiten intercambiar datos; las instalaciones acogen los equipos informáticos y de comunicaciones y las personas operan los elementos citados anteriormente (Gómez y otros, 2012).

Existen activos que dependen unos de otros, por ejemplo los activos esenciales dependen de los equipos, comunicaciones, instalaciones y personas, formándose una

estructura en árbol donde la seguridad de los activos superiores depende de los inferiores, tal como lo menciona Amutio Gómez, y otros (2012) "*esta estructura muestra de arriba hacia abajo las dependencias mientras que de abajo hacia arriba la propagación del daño en caso se materialice la amenaza".*

Según (AEI Seguridad, 2012) un "*activo superior depende de otro activo inferior cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior*". Una vez identificados los activos el siguiente paso es valorarlos, es decir averiguar cuánto vale un activo asignándole un valor de acuerdo al grado de importancia, la valoración según Amutio Gómez, y otros (2012) implica conocer cuan valioso o importante es el activo de información para la continuidad del negocio, permitiendo establecer controles de protección proporcionales al riesgo en las dimensiones de seguridad que sean pertinentes., Areitio Bertolín (2008) menciona que puede ser "*cuantitativa (escala en cantidad numérica) por ejemplo, el rango numérico de 0 a 10, o cualitativa (escala de niveles) por ejemplo: nivel bajo, medio o alto*". Amutio Gómez, y otros (2012) menciona tambien que el valor puede ser propio o acumulado, "*se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos*".

Es de fundamental consideración conocer las consecuencias que acarrearia la materialización de una amenaza, es por ello que se debe calibrar en distintas dimensiones, según Gómez Amutio, y otros (2012), tenemos:

En su disponibilidad, que impacto provocaría no tener o no poder utilizar un activo de información.

En su integridad, que impacto causaría que un activo de información fuese modificado o alterado.

En su confidencialidad, que impacto causaría que la información confidencial fuese conocida o divulgada a quien no debe.

En su autenticidad, que impacto causaría no saber quién accede a un activo de información, es decir saber exactamente quien hace o ha hecho cada cosa.

En su trazabilidad, que daño provocaría no saber quién consume nuestros activos de información, es decir quién hace qué y cuándo.

Luego de identificar los activos de información, se debe identificar y asociar las amenazas a las cuales expuestos pudiendo determinar el nivel de daño que existe e identificar de que amenazas se tratará de proteger en función a la probabilidad de ocurrencia, (Nando, 2010). Las amenazas pueden atacar a un activo en concreto o en cadena por la dependencia existente, Gómez Amutio, y otros (2012) las clasifica así: de origen natural, de origen industrial, errores y fallos no intencionales, y ataques intencionales, (Véase Anexo N° 01). Posterior a ello se procede a valorarlas estimando el porcentaje de degradación y la frecuencia de ocurrencia, la primera hace referencia al porcentaje de daño causado ante de materialización de una amenaza y la segunda a la probabilidad de que se materialice anualmente, todo esto con el fin de estimar el impacto y riesgo potencial de la amenaza sobre el activo, que puede ser cualitativa o cuantitativa.

Cualitativamente, degradación de valor.

MA	Muy Mala	Casi Seguro	Fácil
A	Altas	Muy Alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco Probable	Muy Difícil
MB	Muy Baja	Muy Raro	Extremadamente Difícil

Tabla N° 01 - Degradación del Valor
Fuente: MAGERIT – versión 3.0

Cuantitativamente, se modela numéricamente como una frecuencia de ocurrencia normalmente una tasa anual.

MA	**100**	Muy Frecuente	A Diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco Frecuente	Cada varios años
MB	1/100	Muy Poco Frecuente	Siglos

Tabla N° 02 - Probabilidad de Ocurrencia
Fuente: MAGERIT – versión 3.0

Luego se procede a la estimación del impacto, existen dos tipos, impacto potencial e impacto residual. Según Gomes Armutio, y otros (2012) el impacto potencial es el grado o nivel de daño que se origina sobre un activo de información derivado de la materialización de una amenaza. Es decir, es el grado de exposición del sistema

teniendo en cuenta el valor de los activos de información y las amenazas, pero no los controles de protección actualmente implementados. Para determinar el impacto residual se debe tener en cuenta el valor de los activos de información, el porcentaje de degradación de valor y la eficacia de los controles de protección actualmente implementadas, además nos permite determinar las salvaguardas o controles necesarios para su implementación.

Según Gomes Armutio, y otros (2012) si el valor residual es igual al potencial, entonces los controles no son eficaces, es decir no porque su implementación haya sido en vano sino porque no cumplen o hacen funciones elementales. Para ello se debe redactar el informe de vulnerabilidades identificando las mismas y detallando la relación de lo que debería hacer y lo que no se ha hecho.

Posterior a ello valoramos el riesgo, para Gómez Amutio, y otros (2012) es la estimación del grado de exposición de la materialización de una amenaza o en otras palabras lo que podría pasarles a los activos sino se protegieran adecuadamente, existen 5 niveles de riesgo bajo, medio, alto, muy alto y crítico. Tenemos dos tipos de riesgo, potencial y residual, para la estimación del primero según Gómez Amutio, y otros (2012) se debe tener en cuenta el impacto de las amenazas sobre los activos y la probabilidad de ocurrencia de las amenazas. El cálculo del riesgo residual es sencillo, Gómez Amutio, y otros (2012) menciona que como los activos y sus dependencias no han cambiado, sino solamente la magnitud de la degradación de valor y la probabilidad de ocurrencia de las amenazas, los cálculos de riesgo serán los mismos usando el impacto residual y la probabilidad de ocurrencia residual. (Ver Figura Nº 02).

Figura Nº 02 – Tabla de Valoración de Riesgo
Fuente: MAGERIT – versión 3.0

Para protegernos del riesgo se definen salvaguardas o controles que son procedimientos o tecnologías que reducen el nivel riesgo, influyen en el cálculo del riesgo reduciendo la probabilidad de ocurrencia de las amenazas, llamadas preventivas que pueden llegar a impedir la materialización de una amenaza; y limitando el daño causado, en cualquiera de estas situaciones la amenaza se materializa, pero se limitan sus consecuencias. Según Gómez Amutio, y otros (2012) es importante relativizar los riesgos y solamente centrarse en lo más importante es decir máximo impacto y máximo riesgo, obviando los datos secundarios o despreciables.

Según Areitio Bertolín (2008) los riesgos nunca se eliminan completamente, sólo se mitigan, minimizan y controlan por lo tanto es recomendable planificar no sólo la prevención ante un problema adoptando controles de protección sino también planificar la recuperación en caso alguna amenaza se materialice.

Una vulnerabilidad es toda debilidad del sistema que facilita el éxito de una amenaza potencial, según Seacord y otros (2005) comprender las vulnerabilidades es *"fundamental para entender las amenazas que representan",* para identificar las vulnerabilidades según Jara, y otros (2012) se realiza a partir de escaneos sistemáticos de vulnerabilidades, por ejemplo Nessus o QualysGuard, *además de la criticidad de la vulnerabilidad identificada, depende también del activo que se ve afectado",* es decir aunque la misma vulnerabilidad afecte a varios equipos, la priorización dependerá del valor que represente éste a la organización. En este estudio identificaremos las vulnerabilidades lógicas haciendo uso de herramientas de escaneo del hacking, para las vulnerabilidades físicas nos interesa identificar los puntos de acceso y las zonas vulnerables.

La fase de escaneo para Jara, y otros (2012) es algo más técnico, se basa en la identificación de servicios y aplicaciones que se están ejecutando en el sistema permitiendo aprovechar cualquier vulnerabilidad que pueda explotarse, en otras palabras en esta fase se encuentran todas las fallas, debilidades, errores de configuración, etc., de la red y/o sistema operativo. Por ejemplo, tal como lo menciona Jara, y otros (2012), si nos centramos en un Sistema Operativo es recomendable identificar no sólo la plataforma sino también la familia, es decir conocer si el sistema

es Microsoft o Unix, si es Windows 2003 o 2008, si tiene la última versión de pack instalada, etc.

Con respecto a las aplicaciones el autor nos menciona que el objetivo es identificar el servicio que está corriendo, sobre qué aplicación y cual su versión. Por ejemplo, si tenemos un equipo ejecutando un servidor web, habrá que determinar si es Apache o Internet Information Server y luego la versión del servidor, (Jara y otros, 2012).

Tal como lo menciona Jara, y otros (2012) es necesario conocer a nuestro objetivo para explotar todas las vulnerabilidades existentes, para ello haremos uso de las distintas técnicas de escaneo, teniendo en cuenta el servicio, la plataforma, el sistema operativo, las aplicaciones, etc. que se estén ejecutando en ese momento.

Los autores Jara, y otros (2012) establecen una metodología de 7 pasos secuenciales, de tal manera que la salida de uno sea la entrada del siguiente.

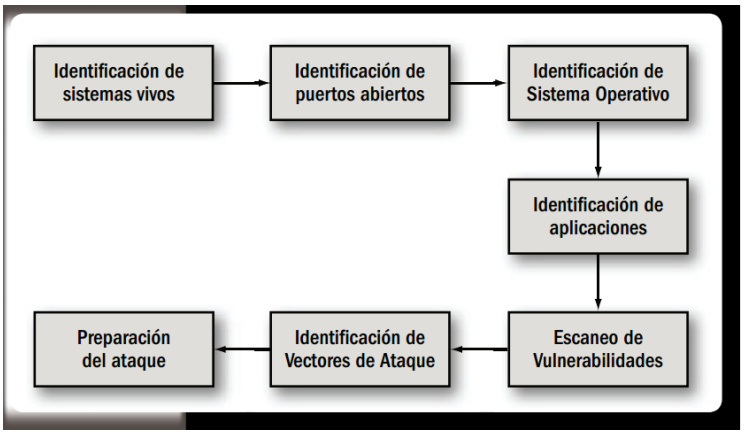


Figura Nº 03 - Metodología de Escaneo
Fuente: Ethical Hacking 2.0

El escaneo de vulnerabilidades según Pacheco G., y otros (2009), nos permite identificar debilidades o deficiencias, *tanto del sistema operativo, como de las aplicaciones* o servicios que se ejecutan. Existen herramientas como QualysGuard, SAINT y Nessus, en el presente estudio se hizo uso de este último para el escaneo de vulnerabilidades lógicas en los ordenadores, tal como lo menciona Chicano Tejada 2015, su funcionamiento es simple "*escanea los puertos para detectar aquellos que están abiertos e intenta enviar ataques a dichos puertos para identificar sus*

vulnerabilidades", una vez detectadas emite un informe mostrando la descripción de la vulnerabilidad y su posible solución.

Es importante evaluar también la seguridad del modelo OSI *(Open System Interconnection)*, según Aguilera López (2011), es "*un modelo que define los niveles o capas de hardware y software de las redes de comunicaciones por donde circula la información"*. Esta información puede verse vulnerada ya que "*atraviesa las mismas capas de manera inversa desde el punto de vista del emisor y receptor*" (Aguilera López, 2011), ante esta debilidad *se aplican medidas de protección evitando la materialización de amenazas* que puedan ser explotadas por un atacante.

Este modelo conceptual consta de 7 capas, las cuatro primeras enfocadas hacia la red y las 3 últimas enfocadas al usuario. Según Alejandro Corletti Estrada (2011) menciona que cada capa debe ser autónoma, es decir no depender de las acciones de otros niveles, el autor define el objetivo principal de los niveles del modelo OSI en la siguiente Figura Nº 04.

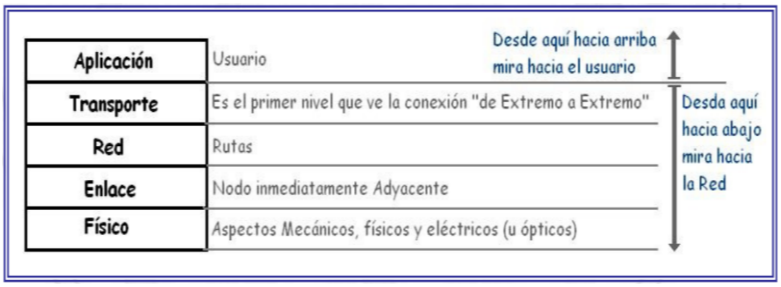


Figura Nº 04 – Capas del Modelo OSI
Fuente: Seguridad por Niveles

La variable de estudio responde a las siguientes interrogantes:

- ¿Cuál es el análisis y valoración de riesgo de la infraestructura tecnológica en el segundo local del Gobierno Regional Piura usando la metodología MAGERIT?
- ¿Cuál es el nivel de importancia y la dependencia de activos en el segundo local del Gobierno Regional Piura?
- ¿Cuáles son las amenazas a las que están expuestos los activos identificados en el segundo local del Gobierno Regional Piura?

- ¿Cuáles son las vulnerabilidades lógicas en el segundo local del Gobierno Regional Piura?
- ¿Cuál es el impacto de un activo derivado de la materialización de una amenaza en el segundo local del Gobierno Regional Piura?
- ¿Cuál es el riesgo de la materialización de una amenaza en el segundo local del Gobierno Regional Piura?
- ¿Cuáles son las salvaguardas en el segundo local del Gobierno Regional Piura?

La elaboración del presente estudio se realiza con el fin de aportar información útil tanto a la Dirección de Oficina de Tecnologías de la Información (OTI) como a la Oficina Regional de Control Interno (ORCI), dando a conocer de forma detallada los riesgos de la infraestructura tecnológica que actualmente presenta el segundo local del Gobierno Regional Piura, pudiendo tomar medidas preventivas a las amenazas y vulnerabilidades identificadas en cada uno de los activos estudiados, contribuyendo a la mejora de la seguridad de la información.

III. METODOLOGÍA

3.1. Tipo y diseño de la investigación

3.1.1. Tipo de estudio

El tipo de estudio es descriptivo, mediante la recopilación de información y análisis de datos se determina la realidad respecto a riesgos y controles de seguridad de la información.

Según Alba E. Fernández A. Manchado C. Tenorio S. (2010), el estudio descriptivo permite conocer situaciones a través de descripciones de actividades, procesos y personas. El objetivo no sólo es la recolección de datos sino poder determinar con qué frecuencia sucede algo.

3.1.2. Diseño del estudio

El diseño es descriptivo simple, se busca y recoge la información de forma directa para tomar decisiones, basado en el análisis de los equipos de trasmisión de datos (ETD), de los activos, las amenazas y vulnerabilidades para luego valorarlas y proponer recomendaciones de acuerdo al análisis de riesgo.

O----------M

Dónde,

O: Observación a través de instrumentos.

M: Población de la cual se recogió información.

3.2. Variables y operacionalización

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
Análisis de Riesgo	*"Proceso consistente en identificar los peligros que afectan a la seguridad, determinar su magnitud e identificar las áreas que necesitan salvaguardas, la valoración de los riesgos es el resultado del proceso del análisis de riesgos"*, (Areitio Bertolín, 2008).	Los indicadores de la dimensión activos de información fueron medidos usando guías de observación que permitieron su registro y valoración. En la dimensión amenazas se usaron guías de observación en paralelo con la de activos de información. De la misma manera se usaron guías de observación en la dimensión salvaguardas, que permitieron el registro de las mismas y su valoración. En las dimensiones de Riesgo e Impacto se usaron guías de observación donde se anotaron la valoración de las mismas. En la dimensión escaneo de vulnerabilidades sus indicadores fueron medidos por guías de observación permitiendo el registro del tipo de vulnerabilidades con o sin exploit y sistema operativo.	Activos de Información	Identificación de Activos de Información	Nominal
				Valoración de Activos de Información	Nominal
			Amenazas	Identificación de Amenazas	Nominal
				Probabilidad de Ocurrencia	Nominal
				Nivel de Degradación de Valor	Nominal
			Salvaguardas	Identificación de Salvaguardas	Nominal
				Tipo de Salvaguardas	Nominal
			Riesgo	Valoración de Riesgo Potencial	Nominal
				Valoración de Riesgo Residual	Nominal
			Impacto	Valoración del Impacto Potencial	Nominal
				Valoración del Impacto Residual	Nominal
			Escaneo de Vulnerabilidades	Tipo de Vulnerabilidades	Nominal
				Tipo de Sistema Operativo	Nominal
				Porcentaje de vulnerabilidades con exploit	Nominal

3.3. Población, muestra y muestreo

Según el inventario realizado el mes de Febrero del presente año, el Gobierno Regional Piura posee una población de 592 activos tecnológicos, de los cuales 404 son ordenadores, para el presente estudio se optó por seleccionar una muestra de 348 activos. La selección de ordenadores fue de la siguiente forma, se hizo uso el software Nessus y se escaneo las 130 primeras IP de la subred (172.16.11.1 - 172.16.11.130) y 30 de la subred perteneciente a servidores (172.16.8.1 - 172.16.8.30), dando un total de 160 ordenadores analizados, los otros activos de Comunicación, Soporte de Información, Equipos Auxiliares, etc. se tomaron en su totalidad.

Objetos	Población	Muestra
Activos de Información del segundo local del GRP	592	348

3.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

3.4.1. Técnicas e instrumentos

Los instrumentos y técnicas que se utilizaron en la recolección de datos fueron aplicados en cada fase de la metodología.

Para conocer el diagnóstico situacional de la organización se hizo uso de una encuesta aplicada a los colaboradores del Segundo local del Gobierno Regional Piura con el fin de determinar la Disponibilidad, Integridad y Confidencialidad de datos, así como la importancia de uso de los sistemas gubernamentales y amenazas a las que está expuesta la oficina donde labora, se aplicaron 77 encuestas a involucrados de las oficinas de Licitaciones, Gerencia de Desarrollo Social, Desarrollo Institucional, Abastecimiento, Contabilidad, Tesorería, Administración, CPAD, Dirección de Obras, Dirección de Estudios y Proyectos, MINDES y PAS. Estos datos sirvieron para dar inicio a la primera fase de la metodología MAGERIT, la identificación y valoración de los activos de información. Para la identificación de los activos se hizo uso de una guía de observación (hoja de registro) donde se anotaron los activos tecnológicos clasificados por capas (Activos Esenciales, Servicios Internos, Equipamiento, Soporte de Información, Instalaciones y Personas), la valoración de los activos se hizo en 5 dimensiones de

Seguridad de la Información Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad permitiendo identificar el valor o la importancia de estos para la organización.

En la dimensión Amenazas se hizo uso de una guía de observación (hoja de registro) donde se anotaron todas las amenazas a las que están expuestas los activos, luego en función de la probabilidad de ocurrencia se determinó de que amenazas se protegerán a los activos, igualmente se valoran en las 5 dimensiones de seguridad teniendo en cuenta el nivel de degradación de valor. En la dimensión Escaneo de Vulnerabilidades se hizo uso de la herramienta Nessus v6.4.3 para la identificación de vulnerabilidades de 160 ordenadores incluyendo servidores, los reportes del mismo software ayudaron directamente en los 3 indicadores Tipo de Vulnerabilidades, Tipo de Sistema Operativo y Porcentaje de Vulnerabilidades con Exploit, para la representación gráfica de este último se hizo uso de la hoja de cálculo de Excel de la Suite de Microsoft, cabe recalcar que el porcentaje se determinó del total de vulnerabilidades con exploit activo, es decir de aquellas que existe un pequeño software para su explotación, además de la Probabilidad de Ocurrencia.

Para las dimensiones de Salvaguardas y Riesgo se hizo uso de guías de observación (hoja de registro) para la anotación de las Salvaguardas, y Valoración del Riesgo en las 5 dimensiones de seguridad teniendo en cuenta la Probabilidad de Riesgo Potencial.

3.4.2. Validez y confiabilidad

Las guías de observación utilizadas en el presente estudio fueron tomadas directamente de la metodología MAGERIT, por lo tanto no necesitan ser sometidas a un proceso de validación, ya que esta metodología ha sido validada internacionalmente y sus instrumentos de recolección de datos son adaptables a la realidad estudiada.

3.5. Métodos de análisis de datos

El análisis de datos se hizo mediante una estadística descriptiva simple que permite representar en histogramas de frecuencia y gráficos de barra los resultados obtenidos. Se usó la herramienta Nessus v6.4.3 para la identificación de

vulnerabilidades lógicas en los ordenadores del cual se obtuvieron informes detallados del tipo de vulnerabilidades y la descripción de la misma. Para la identificación y valoración cuantitativa de activos, amenazas, impacto, riesgo y salvaguardas se usó la hoja de cálculo de Excel perteneciente a la Suite de Microsoft, la cual permitió generar gráficos y análisis de los mismos.

La valoración de los activos se hizo de forma cuantitativa teniendo en cuenta el grado de importancia para la organización, la valoración de las amenazas se hizo de acuerdo a la probabilidad de ocurrencia y nivel de degradación de valor para ello se utilizó una tabla de valoración del 1 al 5, el cálculo del impacto potencial se realizó con la valoración de los activos y la valoración del nivel de degradación de las amenazas, el valor fue la media de ambos valores, el cálculo del impacto residual se obtuvo teniendo en cuenta el valor de los activos, la valoración del nivel de degradación de las amenazas y las salvaguardas actualmente implementadas, el valor fue la media de ambos valores, el cálculo del riesgo potencial se obtuvo tomando en cuenta la tabla de valoración que propone la metodología en función de la probabilidad de ocurrencia y el impacto potencial, el cálculo del riesgo residual se obtuvo del impacto residual y la probabilidad residual de ocurrencia, el valor se obtiene de la misma forma que el riesgo potencial.

3.6. Aspectos éticos

El investigador es responsable de la seriedad y veracidad de los resultados, la privacidad de los datos e información analizada y el respeto por la propiedad intelectual.

IV. RESULTADOS

Cumpliendo con los objetivos planteados en el presente estudio se presentará a continuación el análisis de resultados obtenidos en las distintas fases de la metodología.

De 38 activos de información seleccionados por su nivel de importancia y valorados en las diferentes dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad tenemos que el 34% de activos se encuentran en un nivel de riesgo potencial alto, esto se debe a que el impacto de las amenazas en la capa de datos esenciales, servicios internos, equipos y comunicaciones tienen una probabilidad de ocurrencia posible (Nivel 3) es decir con una frecuencia de ocurrencia de una vez al año y con un 66% indicando un nivel de criticidad de riesgo muy alto (Nivel 4) se encuentran activos de las capas de servicios esenciales, servicios internos, aplicaciones, equipos, comunicaciones, soporte de información, e instalaciones, esto se debe a que las amenazas evaluadas en las distintas dimensiones varían en un nivel de degradación de valor alto y muy alto por ende su nivel de probabilidad e impacto es mucho mayor.

Por ejemplo, tenemos que la capa de comunicaciones y equipos son los activos inferiores más importante en la dimensión disponibilidad con niveles de valoración 4 (Alto) y 5 (Muy alto) en cuanto a degradación de valor y probabilidad de ocurrencia de las amenazas, lo que significa que la negación o la ausencia de los mismos afectaría en grandes proporciones a la organización.

Dato que se confirma con la encuesta aplicada a los involucrados donde muestra que el 96% hace uso de los sistemas gubernamentales como el SIAF, SIGA, CPRESU, mail y portal electrónico para su desempeño laboral diario. (Véase Gráfico Nº01).

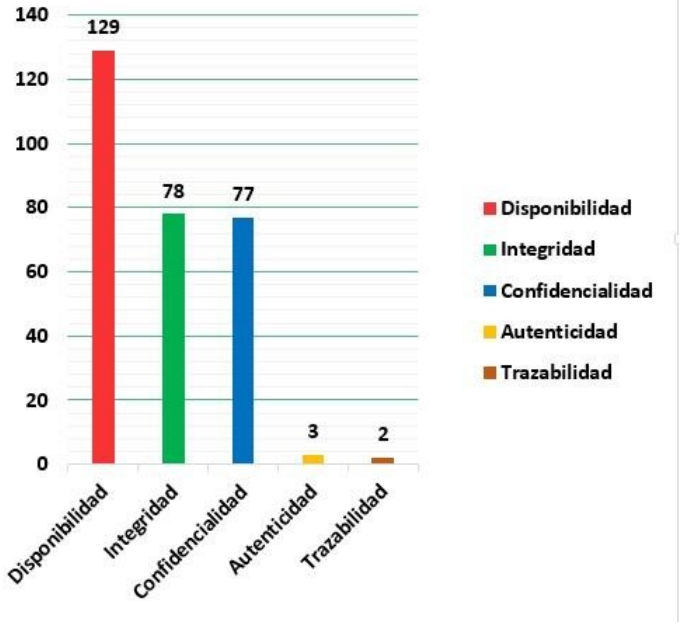
Gráfico N° 1: Porcentaje de Activos Informáticos en Riesgo Potencial

Fuente: Gobierno Regional Piura

Autor: Delgado Mena Javier Eduardo

En el gráfico Nº 02 observamos que la dimensión con mayor número de amenazas es la de disponibilidad, con un total de 129 amenazas de las 159 consideradas en el estudio, por lo contrario con 3 y 2 amenazas respectivamente las dimensiones de autenticidad y trazabilidad, esto se debe porque ante la materialización de una amenaza tendrían una gran probabilidad de causar la indisponibilidad de los servicios y equipos informáticos en general. La amenaza con mayor nivel de degradación de valor (Muy Alta) en esta dimensión, es la de fuego en las capas de equipos y comunicaciones, perteneciente a la categoría de amenazas de origen industrial, es decir la posibilidad de que el fuego acabe con los recursos informáticos, y con menor nivel de degradación de valor en la dimensión disponibilidad, pero la más frecuente encontramos la amenaza uso no previsto es decir el uso de los recursos del sistema con fines de interés personal.

Gráfico N° 02: Número de Amenazas por Dimensión



Fuente: Gobierno Regional Piura

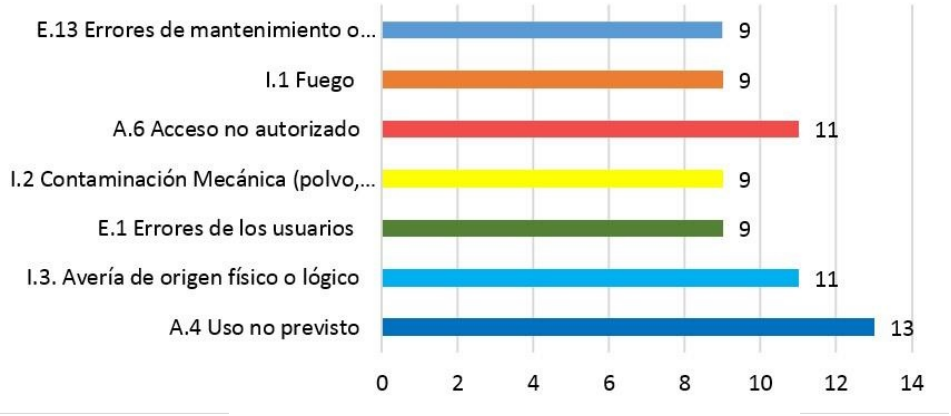
Autor: Delgado Mena Javier Eduardo

De las 159 amenazas consideradas en los activos relevantes, la amenaza más frecuente es el uso no previsto perteneciente a la categoría de ataques intencionales, esto se debe a que muchos de los activos identificados en el Gobierno Regional Piura son utilizados con fines de interés personal, consultas personales en internet, almacenamiento de datos personales, etc. y con menos frecuencia pertenecientes a la categoría de origen industrial y errores y fallos no intencionales, las amenazas de errores de mantenimiento o actualización de equipo (hardware), fuego, contaminación mecánica (polvo, suciedad) y errores de los usuarios.

Esta amenaza representa mayor nivel de degradación de valor en la capa de aplicaciones debido al uso de recursos de manera personal. Algunas de las situaciones comunes realizadas por los usuarios es ejecutar archivos de sus discos extraíbles sin dejar que culmine el escaneo del antivirus corporativo Kaspersky, de esta manera el ordenador o el sistema operativo es amenazado por virus informáticos y con ello la ralentización de los procesos, la indisponibilidad de controladores o en el peor de lo casos del ordenador. Las dimensiones que se verían afectadas son la integridad y la confidencialidad, la primera por el objetivo de los virus (alterar o modificar archivos

del sistema) y la segunda porque información importante quedaría visible a personas no autorizadas. (Véase Gráfico Nº03).

Gráfico N° 3: Amenazas más frecuentes

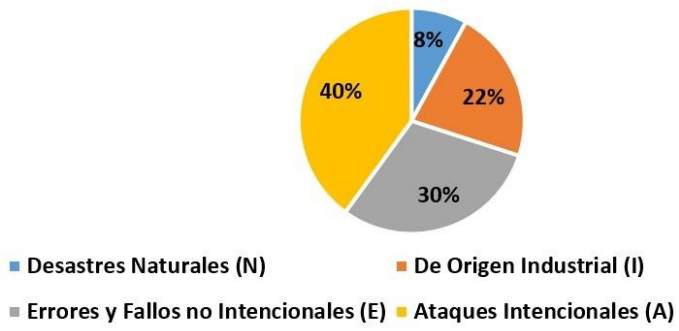


Fuente: Gobierno Regional Piura

Autor: Delgado Mena Javier Eduardo

De las 4 categorías de amenazas consideradas en el estudio, las más frecuentes son del tipo ataques intencionales, debido a que el factor humano influye mucho en ello, tal como se mostró en el Gráfico Nº 03 las más frecuentes son el uso no previsto y acceso no autorizado, seguida de la categoría errores y fallos no intencionales donde también influye el ser humano, entre las más frecuentes encontramos los errores de los usuarios, errores de administrador y errores de mantenimiento o actualización de equipos. (Véase Gráfico Nº04).

Gráfico N° 4: Amenazas más frecuentes por categoría

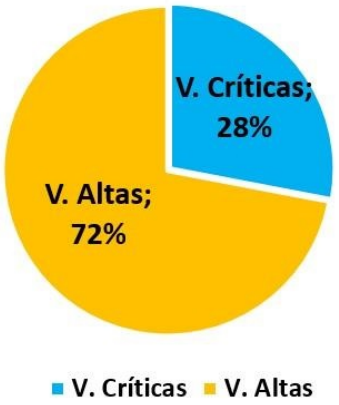


Fuente: Gobierno Regional Piura

Autor: Delgado Mena Javier Eduardo

Del total de ordenadores analizados en el segundo local del Gobierno Regional Piura, la vulnerabilidad más frecuente son las de criticidad alta con un 72%, mientras que la menos frecuente con un 28% las críticas, entre las vulnerabilidades de nivel alto detectadas por el software Nessus v6.4.3 encontramos la desactualización de ficheros del sistema entre los más comunes Flash Player, Microsoft Office, Adobe Reader, Net Framework, entre otros. Por otro lado, entre las vulnerabilidades críticas encontramos vulnerabilidades en DNS, Java, Kaspersky, red de Windows, etc. (Véase Gráfico Nº05).

Gráfico N° 5: Porcentaje de Vulnerabilidades Críticas y Altas



Fuente: Gobierno Regional Piura

Autor: Delgado Mena Javier Eduardo

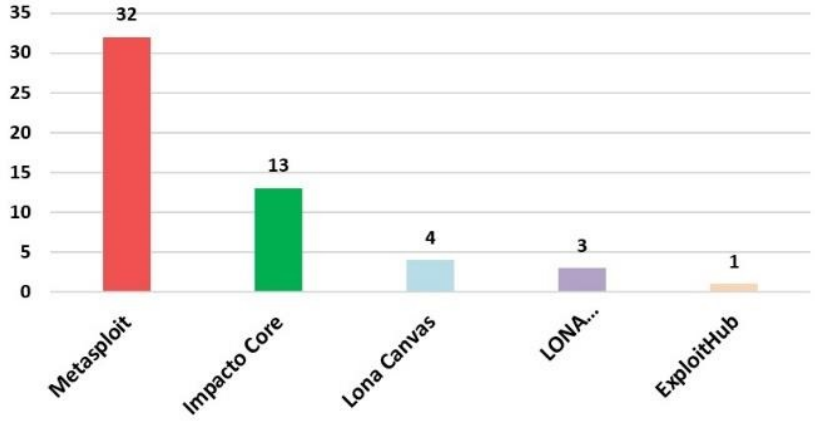
Del total de ordenadores analizados por el software Nessus v6.4.3 tenemos que para el 50 % de vulnerabilidades existen Exploit documentados para su ejecución de los cuales 32 pertenecen a la más grande comunidad de exploit “Metasploit”, esto se debe a que los ordenadores analizados presentan muchas desactualizaciones de ficheros tanto del sistema operativo como de las aplicaciones o servicios instalados. (Véase Gráfico Nº06 y Nº07).

Gráfico N° 6: Porcentaje de Vulnerabilidades con Exploit Activo

Fuente: Gobierno Regional Piura

Autor: Delgado Mena Javier Eduardo

Gráfico N° 7: Exploit Activos



Fuente: Gobierno Regional Piura

Autor: Delgado Mena Javier Eduardo

V. DISCUSIÓN

El presente estudio se llevó a cabo con la finalidad de identificar y valorar el riesgo presente en los activos tecnológicos del Gobierno Regional Piura, se buscó teorías que respalden la investigación, consultándose varias literaturas tomadas como referencia.

Amutio Gómez y otros (2012) en la metodología MAGERIT menciona que la dependencia de activos crea una estructura "*que muestra de arriba hacia abajo las dependencias mientras que de abajo hacia arriba la propagación del daño en caso se materialice la amenaza*", esto se ve contrastado en la medida que los activos inferiores son los más vulnerables y con mayor nivel de riesgo, estos son usados por los usuarios y en la mayoría de casos son la base para el funcionamiento de los demás activos por ejemplo tenemos el activo esencial Internet, si alguna amenaza afectara su disponibilidad todas las ramas superiores que incluye los Sistemas Gubernamentales y que son transversales a todas las áreas (SIGEA, el SIAF o el SIGA) quedarían fuera de red y por lo tanto con disponibilidad nula. Cabe recalcar que estos sistemas gubernamentales son esenciales para el desarrollo laboral diario de los colaboradores.

Se confirma la necesidad de sólo trabajar con los activos relevantes y con estos sus amenazas, impacto y riesgo potencial, tal como lo menciona Amutio Gómez y otros (2012) en la metodología MAGERIT, capítulo 8 de Consejos Prácticos.

Gaona Vásquez (2012) en su investigación indica que el activo con mayor riesgo es el Internet, en la presente investigación tenemos el Internet es el activo inferior de mayor importancia en la dimensión disponibilidad, la materialización de amenazas en este activo afectaría la disponibilidad de los activos de la capa servicios esenciales de la organización, especialmente a los sistemas gubernamentales que son esenciales para el desarrollo laboral diario de los colaboradores. Por otro lado la capa con mayor nivel de riesgo en la investigación según los resultados de la autora es la de aplicaciones con valores de nivel 4 (Muy Alto) en la dimensión disponibilidad y confidencialidad, mientras que los resultados del presente estudio muestran que la capa con mayor nivel de riesgo es la de equipos con niveles de criticidad muy alto en las dimensiones de disponibilidad e integridad y nivel alto en confidencialidad, esto debido a las amenazas como uso no previsto, fuego, errores de mantenimiento, contaminación mecánica son muy frecuentes en los activos.

Se contrasta positivamente con lo que dice Areitio Bertolín (2008) en su libro Seguridad de la Información. Redes, Informática y Sistemas de Información " *los riesgos se pueden minimizar, pero nunca eliminar completamente, por lo que será recomendable planificar, no sólo la prevención ante un problema sino también la recuperación en caso se produzca*". Esto se ve reflejado en que algunas amenazas no tienen salvaguardas suficientes para garantizar su disponibilidad, por ejemplo el acceso no autorizado a la red WIFI, si bien es cierto existen controles activos de filtrado MAC resulta muy fácil y en muy pocos pasos acceder a la red con un sistema operativo GNU/Linux que tenga instalado la suite Aircrack.

Aguilera López (2010), en su libro Seguridad Informática, menciona que el mayor problema de las organizaciones respecto a la pérdida de información, es el factor humano. Esta teoría se pudo contrastar en el análisis del Gráfico Nº 03 donde se comprueba que las amenazas más frecuentes son del tipo ataques intencionales y errores y fallos no intencionales donde influye directa o indirectamente el ser humano, representando un 40% y 30% respectivamente.

VI. CONCLUSIONES

1. De 38 activos de información seleccionados por su nivel de importancia y valorados en las diferentes dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad tenemos que el 66% de activos de información, indicando un nivel de criticidad de riesgo muy alto (Nivel 4) se encuentran los activos de las capas de servicios esenciales, servicios internos, aplicaciones, quipos, comunicaciones, soporte de información, e instalaciones, esto se debe a que las amenazas evaluadas en las distintas dimensiones varían en un nivel de degradación de valor alto y muy alto.

2. La capa con mayor nivel de riesgo es la de equipos con niveles de criticidad muy alto en las dimensiones de disponibilidad e integridad y nivel alto en confidencialidad, esto debido a las amenazas como uso no previsto, fuego, errores de mantenimiento, contaminación mecánica son muy frecuentes en los activos.

3. La capa de comunicaciones y equipos son los activos inferiores más importante en la dimensión disponibilidad con niveles de valoración 4 (Alto) y 5 (Muy alto) en cuanto a degradación de valor y probabilidad de ocurrencia de las amenazas, lo que significa que la negación o la ausencia de los mismos afectaría en grandes proporciones a la organización.

4. Las amenazas más frecuentes son del tipo ataques intencionales y errores y fallos no intencionales donde influye directa o indirectamente el ser humano, representando un 40% y 30% respectivamente. Tal como lo menciona Aguilera López (2010), el mayor problema de las organizaciones respecto a la pérdida de información, es el factor humano.

5. La dimensión más afectada por las amenazas es la de disponibilidad, con un total de 129 amenazas de las 159 consideradas en el estudio, es decir, la materialización de las mismas tendría una gran probabilidad de causar la indisponibilidad de los servicios y equipos informáticos en general. La amenaza con mayor nivel de degradación de valor (Muy Alta) en esta dimensión, es la de fuego en las capas de

equipos y comunicaciones, es decir la posibilidad de que el fuego acabe con los recursos informáticos.

6. El 72% de las vulnerabilidades lógicas detectadas con el software Nessus v6.4.3, son de criticidad alta y el 50% del total de las vulnerabilidades tienen exploit para su ejecución.

VII. RECOMENDACIONES

1. Realizar una investigación que permita realizar la Gestión de Riesgos a partir del análisis de riesgo realizado en el presente estudio.

2. Realizar una investigación que permita analizar las amenazas y vulnerabilidades en todas las capas del modelo OSI de la arquitectura de red del Gobierno Regional Piura.

3. Realizar un proyecto que permita gestionar la ubicación y organización del Data Center basados en normas ISO u otros estándares internacionales, garantizando la funcionalidad, disponibilidad e integridad del mismo.

4. Realizar un proyecto de software que permita automatizar los procesos o fases del análisis de riesgo que propone la metodología MAGERIT.

VIII. PROPUESTA

8.1. Propósito

El análisis de riesgo de la infraestructura tecnológica se llevó a cabo con la finalidad de identificar los activos relevantes para la organización, determinar las amenazas a las que están expuestos estos activos y estimar el nivel de impacto de la materialización de las amenazas y el nivel de riesgo de los activos.

Para la identificación de las vulnerabilidades lógicas se utilizó la herramienta de escaneo Nessus v6.4.3, la cual permitió generar reportes detallados sobre el tipo de vulnerabilidades, tipo de Sistema Operativo y Vulnerabilidades con Exploit.

8.2. Ámbito del análisis de riesgo

El análisis de riesgo consiste en identificar los peligros que afectan la seguridad de la información, determinar su magnitud y las áreas que necesitan salvaguardas. Por lo tanto, el estudio ha permitido identificar los activos relevantes o importantes para la organización, identificar las amenazas a las cuales están expuestas estos activos y determinar su magnitud (impacto y riesgo), y con ello determinar las salvaguardas para mitigar el impacto de las amenazas.

El producto desarrollado no es solamente el análisis y valoración de riesgo, sino también un Plan de Mantenimiento Preventivo de Equipos Informáticos con el objetivo de identificar y corregir los problemas técnicos antes de que estos provoquen la indisponibilidad del equipo.

8.3. Perspectivas del análisis de riesgo

El análisis de riesgo en el segundo local del Gobierno Regional Piura nace de la necesidad de identificar las amenazas a las cuales están expuestos los activos informáticos de la organización y poder determinar el impacto que provocaría la materialización de estas y el nivel de riesgo de los activos en caso no se protegieran adecuadamente.

Tal como lo dice Nando (2010) "*es muy importante que una organización realice un examen consciente de su actual situación respecto a la seguridad, este análisis permitirá tomar acciones en caso que el resultado indique que se encuentra en una situación comprometida*".

La metodología MAGERIT establece 7 fases para el desarrollo del análisis de riesgo:

- Activos.
- Amenazas.
- Determinación del impacto potencial.
- Determinación del riesgo potencial.
- Salvaguardas.
- Impacto residual.
- Riesgo residual.

8.4. Desarrollo del análisis de riesgo

Fase 01: Activos

1.1. Identificación de activos

Toda organización posee activos y recursos que representan valor y utilidad para la entidad, estos se pueden clasificar en 10 capas: servicios esenciales, datos esenciales, servicios internos, aplicaciones, equipos, comunicaciones, elementos auxiliares, soporte de información, instalaciones y personas.

1.2 Dependencia de activos

Una vez identificados los activos se debe estructurar la dependencia de valor de los mismos, tal como lo menciona Amutio Gómez, y otros (2012) "*esta estructura muestra de arriba hacia abajo las dependencias mientras que de abajo hacia arriba la propagación del daño en caso se materialice la amenaza*", se dice que un activo depende de otro cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior.

1.3 Valoración de activos

Luego de conocer los activos de la organización procedemos a valorarlos en las 5 dimensiones de seguridad de la información (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) es decir averiguar cuánto vale asignándole un valor de acuerdo al grado de importancia, la cual puede ser cualitativa (escala de niveles) por ejemplo: nivel bajo, medio o alto" o

cuantitativa (escala en cantidad numérica) por ejemplo, el rango numérico de 0 a 5.

Fase 02: Amenazas

2.1 Identificación de amenazas

Luego de identificar los activos o recursos que necesitan protección, se debe identificar las amenazas existentes a la que están expuestas estos activos. Posterior a ello se debe determinar de qué amenazas se debe de proteger a los activos en función a la probabilidad de ocurrencia.

Según Gómez Amutio, y otros (2012) las clasifica así: de origen natural, de origen industrial, errores y fallos no intencionales, y ataques intencionales.

2.2 Valoración de amenazas

Procedemos a valorarlas estimando el porcentaje de degradación y la frecuencia de ocurrencia, la primera hace referencia al porcentaje de daño causado ante de materialización de una amenaza, la segunda a la probabilidad de que se materialice una amenaza anualmente, todo esto con el fin de saber el impacto y riesgo potencial de dicha amenaza sobre el activo.

Fase 03: Impacto potencial

El siguiente paso es la estimación del impacto potencial, que es el daño que se origina sobre un activo derivado de la materialización de una amenaza, el valor se obtiene teniendo en cuenta la valoración de los activos y el porcentaje de degradación de las amenazas, pero no las salvaguardas actualmente desplegadas.

Fase 04: Riesgo potencial

Posterior a ello valoramos el riesgo, esta estimación indica lo que podría pasarles a los activos sino se protegieran adecuadamente, existen 5 niveles de riesgo bajo, medio, alto, muy alto y crítico.

Fase 05: Salvaguardas

Para protegernos del riesgo se definen salvaguardas o contramedidas que son procedimientos o tecnologías que reducen el riesgo, entran en el cálculo del riesgo

de dos formas reduciendo la probabilidad de las amenazas, llamadas preventivas pueden llegar a impedir la materialización de una amenaza y limitando el daño causado, en cualquier de estas situaciones la amenaza se materializa, pero se limitan sus consecuencias.

Fase 06: Impacto residual

En los pasos anteriores no se han tomado en cuenta las salvaguardas o controles de seguridad actualmente desplegados, para estimar el impacto residual se debe tener en cuenta la eficacia de las mismas, el valor de los activos y el porcentaje de degradación.

Fase 07: Riesgo residual

La estimación del riesgo residual se obtiene a partir de impacto residual y la probabilidad residual de ocurrencia.

8.5. Fundamentación de las amenazas

8.5.1. Acceso a internet

- Fallos de servicios de comunicaciones: La indisponibilidad del servicio de internet afectaría gravemente el desempeño de las labores diarias de los colaboradores del GRP, debido al uso del correo electrónico, portal web y sistemas gubernamentales.
- Denegación de servicio: Al existir agentes externos conectados a la red, más probable es la ejecución de un DOS o DDOS, incluso si algún agente logra acceder al menos a la cache ARP.

8.5.2. Portal electrónico

- Alteración accidental de la información: Existe una situación peculiar de compatibilidad en los navegadores, la administración del módulo transparencia sólo se puede acceder desde IE con vista de compatibilidad, situación que genera problemas con los usuarios debido a que las acciones de guardar no se habilitan, pero si las de reemplazar y eliminar, situación que se presta para la alteración accidental de la información.

- Repudio: Este principio de la seguridad de la información es útil al momento de determinar quién es el responsable de una o varias acciones ejecutadas en el portal web.

8.5.3. Ofimática

- Uso no previsto: Un gran porcentaje de colaboradores hace uso de las aplicaciones de ofimática para uso personal.
- Vulnerabilidades de los programas: El escaneo realizado con la herramienta Nessus v6.4.3, indica una alta tasa de desactualización de ficheros, la mayoría de ellos con Exploit para su ejecución

8.5.4. Sistema operativo

- Avería de origen físico o lógico: El escaneo realizado con la herramienta Nessus v6.4.3, indica que el 95% de los ordenadores tiene averías lógicas, es decir vulnerabilidades en sus aplicaciones, servicios, puertos, ficheros, etc.
- Difusión de software dañino: Al infectarse un ordenador por alguna memoria extraíble y al estar en red todos los ordenadores, es mucho más probable la difusión del software dañino.
- Vulnerabilidades de los programas: El escaneo realizado con la herramienta Nessus v6.4.3, indica que aplicaciones como Microsoft Office, Adobe Reader, Adobe Flash Player, .Net Framework son algunos de las más vulnerables.
- Errores de mantenimiento o actualizaciones: El escaneo realizado con la herramienta Nessus v6.4.3, indica una alta tasa de desactualización de aplicaciones como de ficheros, actualmente la organización está pasando por situaciones de ataques de virus, esto debido a que el antivirus no es actualizado constantemente en algunas máquinas ya que la administración de este se hace mediante un servidor centralizado.
- Uso no previsto: Introducir memorias USB, discos duros portátiles o el propio celular para el almacenamiento de archivos personales, son algunas de las situaciones que podrían afectar la disponibilidad del Sistema Operativo.

8.5.5. Servidores

- Condiciones inadecuadas de temperatura o humedad: El rango de temperatura óptimo para un Data Center es de 15 °C y 21 °C, actualmente se cuenta con un solo equipo de enfriamiento para toda el área de la Oficina de Tecnologías de la Información.

  Se presenta una propuesta de implementación de un Data Center donde se propone utilizar equipos de aire acondicionado de precisión y un equipo de aire acondicionado comercial como backup.
- Errores de mantenimiento o actualización de equipo (hardware): Debido a la inadecuada temperatura es necesario analizar la vida útil de los equipos, el mantenimiento y cambio de los mismos.
- Destrucción de la información: Los backups de toda la información de los servidores se almacena en un equipo de respaldo que se ubica en la misma oficina a la vista de todos.

8.5.6. WI-FI

- Errores del administrador: Es peligroso no dar de baja a los usuarios externos que se añaden temporalmente, un escaneo de la caché ARP, de las IP y MAC de los servidores, un escaneo de las vulnerabilidades de los mismos, son algunas de las muy pocas acciones que podrían darse en contra de la red.
- Acceso no autorizado: Si bien es cierto se controla el acceso del host mediante filtro MAC, en pocos pasos podemos acceder a la red con un SO GNU/Linux que tenga instalado la suite Aircrack.
- Fallos de servicios de comunicaciones: Al ser un servicio esencial la detención del mismo afectaría el trabajo o las labores de los colaboradores.
- Análisis de tráfico - Interceptación de información: Al no existir medios de encriptación de datos, es sumamente fácil la interceptación y análisis del tráfico de paquetes.
- Suplantación de identidad: Debido al fácil acceso a las computadoras del gobierno regional un ataque de envenenamiento ARP sería muy fácil.

8.5.7. Red de área local

- Acceso no autorizado: El mayor porcentaje de ordenadores conectados a la red usan conexión Ethernet, existiendo muchos puntos de red en las oficinas, la situación problema es que cualquier persona en horarios de refrigerio puede conectar y desconectar los cables para tener conectividad en su portátil, además existen oficinas en las cuales los Switch no están protegidos, por ende, resultaría muy fácil que un usuario lleve un cable de red y conectarlo directamente al Switch.

8.6. Detalle de propuesta

Teniendo en cuenta las amenazas consideradas para cada activo relevante a continuación se dará a conocer a grandes rasgos las salvaguardas pertenecientes a cada activo, específicamente estas son descritas en el Anexo N° 06.

De la capa servicios esenciales tenemos el activo expediente administrativo físico, con sus amenazas errores de usuario, destrucción intencional de la información, fuego entre otros, se propone concienciar a los usuario sobre el uso y ubicación de los expedientes físicos en relación a los puntos eléctricos, como se puede observar en el Anexo N° 05, en muchas oficinas del recinto los documentos se encuentran demasiado cerca de los toma corriente y en el peor de los casos en una oficina el supresor de picos que alimenta los switch está sobre un montón de papeles, generando así la amenaza de que un incendio acabe con los recursos informáticos.

El activo acceso a internet posee la amenaza fallos de servicios de comunicaciones, se propone asegurar la disponibilidad del acceso al mismo, primero haciendo un análisis de cuanto ancho de banda se necesita para una óptima comunicación y transferencia de paquetes, luego cumplir con el mantenimiento preventivo de los Access Point, Router y Switch también propuesto en esta investigación, además de sugerir adquirir al menos un dispositivo de comunicación como reserva en caso la avería e indisponibilidad de un ejemplar.

De la capa aplicaciones tenemos el activo de ofimática la cual tiene como amenazas el uso no previsto, errores de actualización y vulnerabilidades de los programas, se propone la configuración total en los equipos de Windows Update.

El activo sistema operativo tiene como amenazas la difusión de software dañino, vulnerabilidad de los programas, uso no previsto, etc., se propone la actualización de todos los ficheros, software y configuración automática de Windows Update, mitigando así las consecuencias de integridad y disponibilidad de datos, además de crear una cuenta por usuario para la ejecución de Backups en la nube alojadas en servidores gratuitos, mencionando por ejemplo Mega que ofrece 50 GB de almacenamiento, garantizando la disponibilidad de los archivos por el uso no previsto de los recursos.

Los servidores virtuales poseen las siguientes amenazas, ataques informáticos, vulnerabilidades de los programas, denegación de servicio, acceso no autorizado, etc., se propone la instalación de los parches publicados por Microsoft en el caso de Windows Server, garantizar la disponibilidad del servicio implementando honeypot o honeynet con la finalidad de prevenir ataques informáticos y el uso de herramientas de análisis de vulnerabilidades.

De la capa equipos tenemos el activo servidores, poseen amenazas tales como condiciones inadecuadas de temperatura o humedad, degradación de los soportes de almacenamiento de información, errores de mantenimiento de equipos, destrucción de la información, etc., se propone asegurar la disponibilidad de los mismos adquiriendo equipos de enfriamiento, ventiladores directos a la fuente generadora de calor de los mismos y estandarizar la ubicación de los equipos. Debido a la inadecuada temperatura en la actualidad, (cabe mencionar que solo se cuenta con un equipo de aire acondicionado para toda la Oficina de Tecnologías de Información), es necesario analizar la vida útil de los equipos, programar mantenimientos preventivos y el cambio de los mismos. Ver anexo 10 – Propuesta de implementación de un Data Center.

Para las amenazas errores de usuarios, destrucción de la información, condiciones inadecuadas de temperatura, fuego, etc. pertenecientes al activo computadoras de escritorio, se propone concienciar al usuario sobre las consecuencias del software dañino, la importancia del uso de antivirus y con ello el cumplimiento de las directivas del uso de equipos informáticos, además de las consecuencias del acceso no autorizado y las causas probables de fuego causando la pérdida total o parcial de la información y del recurso informático. Se propone además una adecuada

ubicación de las mismas con relación a los equipos de ventilación existentes en cada oficina, en caso no se abasteciera coordinar la adquisición de los mismos, también informar sobre el adecuado uso de los supresores de pico y los estabilizadores.

El activo Access Pont posee las siguientes amenazas, fuego, contaminación mecánica, errores de mantenimiento de equipos, etc., para lo cual se propone asegurar la disponibilidad del mismo primeramente con una correcta ubicación del equipo y ejecutando progresivamente el mantenimiento preventivo de los equipos informáticos.

De la capa comunicaciones el activo WIFI posee las siguientes amenazas, errores del administrados, acceso no autorizado, análisis de tráfico, entre otros, para lo cual se propone una mejor coordinación de bajas de acceso de los usuarios externos, entiéndase por aquellos que solicitan acceso a la red por un determinado tiempo, además de asegurar la disponibilidad de la comunicación con los mantenimientos preventivos a los Access Pont. Se propone también el uso de medios encriptados o de VPN garantizando la integridad de la comunicación y transferencia de archivos entre las distintas oficinas o por lo menos entre los directores de cada área.

El activo red de área local posee las siguientes amenazas, errores del administrador, acceso no autorizado, interceptación de información, etc., para lo cual se propone directivas de uso personal de los puntos de red, gabinetes de pared para la protección de los switch en las oficinas, el uso de medios encriptados o de VPN garantizando la integridad de la comunicación y transferencia de archivos entre las distintas oficinas o por lo menos entre los directores de cada área.

REFERENCIAS

Aceituno Canal, Vicente. 2006. *Seguridad de la informacion/ Information Security: Expectativas, Riesgos Y Tecnicas De Proteccion.* s.l. : Editorial Limusa S.A. De C.V., 2006. pág. 149. ISBN 9681868560, 9789681868567.

AEI Seguridad. 2012. *Protección de Infraestructuras Críticas: guía para la elaboración de Planes de Seguridad del Operador y Planes de Protección Específica.* [ed.] AEI Seguridad. España : AEI Seguridad, 2012. 978-84-615-5789-9.

Aguilera López, Purificación. 2011. *Introducción a la seguridad informática.* s.l. : Editex, 2011. ISBN: 8490031061, 9788490031063.

—. 2010. *Seguridad informática.* s.l. : Editex, 2010. pág. 240. 8497717619.

Alberts, Christopher y Dorofe, Audrey. 2002. *Managing Information Security Risks: The OCTAVE (SM) Approach.* Boston : Addison-Wesley Professional, 2002. ISBN: 978-0-321-11886-8.

Areitio Bertolín, Javier . 2008. *Seguridad de la información. Redes, informática y sistemas de información.* [ed.] Editorial Paraninfo. Madrid : Paraninfo, 2008. 8497325028, 9788497325028.

Baars, Hans, y otros. 2018. *Fundamentos de la seguridad de la información: basado en ISO 27001 e ISO 27002.* s.l. : Brasport , 2018. ISBN: 8574528609, 9788574528601.

Calder, Alan y Watkins, Steve. 2019. *Information Security Risk Management for ISO 27001/ISO 27002.* s.l. : IT Governance Ltd, 2019. ISBN: 1787781372, 9781787781375.

Chen, Pei-yu, Kataria, Gaurav y Krishnan, Ramayya. 2011. Correlated failures, diversification, and information security risk management. 2011, Vol. 35.

Chicano Tejada, Ester . 2015. *Auditoría de seguridad informática. IFCT0109.* s.l. : IC Editorial, 2015. 8416433232, 9788416433230.

Corrales Hermoso, Alberto Luis, Beltrán Pardo, Martha y Guzman Sacristán, Antonio. 2006. *Diseño e implantación de arquitecturas informáticas seguras. Una aproximación práctica.* s.l. : Librería-Editorial Dykinson, 2006. 8499823475, 9788499823478.

Del Peso Navarro, Emilia. 2002. *La seguridad de los datos de caracter personal.* s.l. : Diaz de Santos, 2002. ISBN: 9788479785277.

Diaz Orueta, Gabriel, y otros. 2004. *Seguridad en las comunicaciones y en la información.* s.l. : Editorial UNED, 2004. ISBN: 8436247892, 9788436247893.

Escrivá, Gema, Romero, Rosa y Ramada, David. 2013. *Seguridad Informatica.* s.l. : Macmillan Iberia SA, 2013.

Fisher, Royal. 1988. *Seguridad en los sistemas informáticos.* s.l. : Ediciones Díaz de Santos, 1988. ISBN: 8486251958, 9788486251956.

François Carpentier, Jean. 2016. *La seguridad informática en la PYME: Situación actual y mejores prácticas.* s.l. : Ediciones ENI, 2016. ISBN: 2409001807, 9782409001802.

Gallotti, Cesare. 2019. *Information security: risk assessment, management systems, the ISO/IEC 27001 standard.* s.l. : Lulu.com, 2019. ISBN: 0244149550, 9780244149550.

Gaona Vásquez, Karina del Rocío . 2013. *Aplicación de la Metodología MAGERIT en el Análisis y Gestión de Riesgos de la Seguridad de la Información aplicado a la Empresa Pesquera e Industrial Bravito S.A en la ciudad de Machala.* Machala : s.n., 2013.

García Moran, Jean Paul, y otros. 2011. *Hacking y Seguridad en Internet.* Madrid : Grupo Editorial RA-MA, 2011. ISBN: 9788499640594.

García, Alfonso y Alegre Ramos, Maria del Pilar. 2011. *Seguridad Informática.* Madrid : Parainfo, 2011. ISBN 9788428344555.

Giménez Albacete, José Francisco. 2014. *Seguridad en equipos informáticos. IFCT0109 - Seguridad informática.* España : IC Editorial, 2014. ISXN 9788416271115.

Gómez Fernández, Luis y Andrés Álvarez, Ana. 2012. *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* Madrid. España : AENOR Ediciones (Asociación Española de Normalización), 2012. ISBN: 9788481437492.

Gomez Vieites, A. 2010. *Seguridad Informática. Básico.* s.l. : Starbook Editorial, S.A., 2010. ISBN: 8492650362, 9788492650361.

Gómez Vieites, Alvaro. 2014. *Seguridad en Equipos Informáticos.* Madrid : Grupo Editorial RA-MA, 2014. 9788492650767.

Gómez, Amutio, Miguel, Angel y Candau, Javier. 2012. *MAGERIT - version 3.0 Metodología de Análisis y gestión de Riesgos de los Sistemas de Información.* Madrid : Ministerio de Hacienda y Administraciones Públicas, 2012. NIPO: 630-12-171-8.

Hiles, Andrew. 2000. *Business Continuity: Best Practices.* s.l. : Rothstein Associates, 2000. ISBN-10 : 0964164833; ISBN-13 : 978-0964164833.

Huidobro Moya, José Manuel y Roldan Martinez, David. 2005. *Seguridad en redes y sistemas informáticos.* s.l. : Ediciones Paraninfo, 2005. pág. 336. ISBN-10 : 8428329176; ISBN-13 : 978-8428329170.

Jara, Héctor y Pacheco, Federico G. 2012. *Ethical Hacking 2.0.* Buenos Aires : Fox Andina S.A., 2012. 978-987-1857-63-0.

Kenyon, Bridget. 2019. *ISO 27001 controls – A guide to implementing and auditing.* s.l. : IT Governance Ltd, 2019. ISBN: 1787781453, 9781787781450.

Mejía Londoño, Cesar Augusto, Ramirez Galvis, Nini Johana y Rivera Cardon, Juan Sebastian. 2012. *Vulnerabilidades, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos de las organizaciones.* Colombia : s.n., 2012.

Nando. 2010. *Programa avanzado de estudio: Seguridad en Sistemas de Información.* 2010.

Ortega Candel, José Manuel. 2018. *Hacking ético con herramientas Python.* s.l. : Grupo Editorial RA-MA, 2018. 9788499647319.

Pacheco G., Federico y Jara, Hector. 2009. *Hackers al Descubierto.* s.l. : USERSHOP, 2009. 9876630083, 9789876630085.

Pagliari, Gustavo A. y Eterovic, Jorge. 2012. *Metodología de Análisis de Riesgos Informáticos.* s.l. : Editorial Academica Espanola, 2012. ISBN: 3848471841, 9783848471843.

Probst, Christian , y otros. 2010. *Insiders Threat in Cyber Security.* s.l. : Springer Science & Business Media, 2010, 2010. 1441971335, 9781441971333.

Romero Castro, Martha Irene, y otros. 2018. *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* s.l. : 3Ciencias, 2018. ISBN: 8494930613, 9788494930614.

Schmidt, Walker. 2019. *Una guía completa para principiantes sobre la seguridad de los sistemas de información.* s.l. : Independently Published, 2019. ISBN: 108616332X, 9781086163322.

Watkins, Steve. 2013. *An Introduction to Information Security and ISO27001:2013: A Pocket Guide.* s.l. : IT Governance Publishing, 2013. ISBN: 1849285276, 9781849285278.

Webb, Jeb, y otros. 2014. *A situation awareness model for information security risk management.* Kidlington : Elsevier Advanced Technology, 2014. Vol. 44. ISSN: 0167-4048; 1872-6208.

Zeegers, Ruben. 2018. *Information Security Management Professional based on ISO/IEC 27001.* s.l. : Van Haren, 2018. ISBN: 9401803676, 9789401803670.

Zgavc, Nele, y otros. 2019. *Gestión de Riesgos: Técnicas de Evaluación de Riesgos.* Reino Unido : AENOR, 2019.

Berrío López, J. (2016-02.). *Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001.*

Hernández Enrique. 2003. *Seguridad y privacidad en los sistemas informáticos. [En línea] 2005. http://www.disca.upv.es/enheror/pdf/ACTASeguridad.PDF*

ANEXOS

Anexo 1: Matriz de consistencia

PROBLEMA	OBJETIVOS	VARIABLE	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
General ¿Cuál es el análisis y valoración de riesgo de la infraestructura tecnológica en el segundo local del Gobierno Regional Piura usando la metodología MAGERIT?	**General** Determinar el análisis y valoración del riesgo de la infraestructura tecnológica en el segundo local del Gobierno Regional Piura usando la metodología MAGERIT	V: Análisis de Riesgo	Activos de Información	Identificación de Activos de Información	Nominal
				Valoración de Activos de Información	Nominal
Específicos ¿Cuál es el nivel de importancia y la dependencia de activos en el segundo local del Gobierno Regional Piura?	**Específicos** Determinar el nivel de importancia y la dependencia de activos en el segundo local del Gobierno Regional Piura.		Amenazas	Identificación de Amenazas	Nominal
				Probabilidad de Ocurrencia	Nominal
¿Cuáles son las amenazas a las que están expuestos los activos identificados en el segundo local del Gobierno Regional Piura?	Determinar las amenazas a las que están expuestos los activos identificados en el segundo local del Gobierno Regional Piura.			Nivel de Degradación de Valor	Nominal
			Salvaguardas	Identificación de Salvaguardas	Nominal
¿Cuáles son las salvaguardas en el segundo local del Gobierno Regional Piura?	Identificar las salvaguardas en el segundo local del Gobierno Regional Piura.			Tipo de Salvaguardas	Nominal

PROBLEMA	OBJETIVOS	VARIABLE	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
Específicos ¿Cuál es el impacto de un activo derivado de la materialización de una amenaza en el segundo local del Gobierno Regional Piura? ¿Cuál es el riesgo de la materialización de una amenaza en el segundo local del Gobierno Regional Piura? ¿Cuáles son las vulnerabilidades lógicas en el segundo local del Gobierno Regional Piura?	**Específicos** Estimar el impacto sobre el activo derivado de la materialización de una amenaza en el segundo local del Gobierno Regional Piura. Estimar el riesgo de la materialización de una amenaza en el segundo local del Gobierno Regional Piura. Determinar las vulnerabilidades lógicas en el segundo local del Gobierno Regional Piura.	V: Análisis de Riesgo	Riesgo	Valoración de Riesgo Potencial	Nominal
				Valoración de Riesgo Residual	Nominal
			Impacto	Valoración del Impacto Potencial	Nominal
				Valoración del Impacto Residual	Nominal
			Escaneo de Vulnerabilidades	Tipo de Vulnerabilidades	Nominal
				Tipo de Sistema Operativo	Nominal
				Porcentaje de vulnerabilidades con exploit	Nominal

Anexo 2: Glosario

GLOSARIO

- **Activo de información:** Es todo aquello que representa y posee valor para la organización, puede ser base de datos, archivos físicos, ficheros, aplicaciones o software, equipos informáticos, equipos de comunicaciones, entre otros.

- **Confidencialidad:** Propiedad que determina que la información debe ser accesible sólo por entidades o usuarios autorizados.

- **Integridad:** Propiedad que determina la no modificación o alteración de los activos de información.

- **Disponibilidad:** Propiedad que determina que la información debe estar accesible en el momento que se requiera.

- **Amenaza:** Es cualquier evento no previsto que aprovecha una vulnerabilidad existente en el sistema para materializarse, pueden ser intencionales o accidentales.

- **Vulnerabilidad:** Es toda debilidad o deficiencia existente en el sistema que permite la materialización de una amenaza.

- **Impacto:** Es el nivel de daño que se origina sobre un activo derivado de la materialización de una amenaza.

- **Riesgo:** Es el grado de exposición de la materialización de una amenaza, indica lo que podría pasarles a los activos de información sino se protegieran adecuadamente.

- **Salvaguarda:** Procedimientos o mecanismos de acción que permiten reducir el nivel de riesgo, pueden ser prevención, administración, recuperación, disuasoria o de concienciación.

Anexo 3: Clasificación de amenazas (Magerit)

Desastres naturales (N)

N.1 Fuego

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [D] Disponibilidad
Descripción: Incendios: Posibilidad de que el fuego acabe con recursos del sistema.	

N.2 Daños por agua

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [D] Disponibilidad
Descripción: Inundaciones: Posibilidad de que el agua acabe con recursos del sistema.	

N.* Desastres naturales

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [D] Disponibilidad
Descripción: Otros incidentes sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, etc.	

De origen industrial (I)

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana, pueden ser accidentales o deliberadas.

I.1 Fuego

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [D] Disponibilidad
Descripción: Incendio: Posibilidad de que el fuego acabe con los recursos del sistema. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.2 Daños por agua

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [D] Disponibilidad
Descripción: Escapes, fugas, inundaciones: Posibilidad de que el agua acabe con recursos del sistema. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.* Desastres industriales

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [D] Disponibilidad
Descripción: Otros desastres debidos a la actividad humana: explosiones, derrumbes, etc. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.3 Contaminación mecánica

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [D] Disponibilidad
Descripción: Vibraciones, polvo, suciedad, etc. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.4 Contaminación electromagnética

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar	1. [D] Disponibilidad
Descripción: Interferencias de radio, campos magnéticos, luz ultravioleta, etc. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.5 Avería de origen físico o lógico

Tipos de Activos	Dimensiones
[SW] Aplicaciones (software) [HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar	1. [D] Disponibilidad
Descripción: Fallos en los equipos o en los programas. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.6 Corte del suministro eléctrico

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar	1. [D] Disponibilidad
Descripción: Cese de la alimentación de potencia. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.7 Condiciones inadecuadas de temperatura o humedad

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar	1. [D] Disponibilidad
Descripción: Deficiencias en la aclimatación de los locales, excesivo calor, excesivo frío, exceso de humedad, etc. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.8 Fallo de servicios de comunicaciones

Tipos de Activos	Dimensiones
[COM] Redes de Comunicaciones	1. [D] Disponibilidad
Descripción: Cese de la capacidad de transmitir datos de un sitio a otro, por destrucción física de los medios o incapacidad para atender el tráfico. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.9 Interrupción de otros servicios y suministros esenciales.

Tipos de Activos	Dimensiones
[AUX] Equipamiento Auxiliar	1. [D] Disponibilidad
Descripción: Otros servicios o recursos necesarios para la operación de los equipos, papel, tóner, refrigerante, etc. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.10 Degradación de los soportes de almacenamiento de la información

Tipos de Activos	Dimensiones
[Media] Soportes de Información	1. [D] Disponibilidad
Descripción: Como consecuencia del paso del tiempo. Origen: Entorno (accidental). Humano (accidental o deliberado).	

I.11 Emanaciones electromagnéticas

Tipos de Activos	Dimensiones
[HW] Equipos Informáticos [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [D] Disponibilidad
Descripción: Hecho de poner vía radio datos internos a disposición de terceros, es una amenaza donde el emisor es víctima pasiva de ataque. Origen: Entorno (accidental). Humano (accidental o deliberado).	

Errores y fallos no intencionales (E)

E.1 Errores de los usuarios

Tipos de Activos	Dimensiones
[D] Datos / Información [Keys] Claves Criptográficas [S] Servicios [Media] Soportes de Información [SW] Aplicaciones (software)	1. [I] Integridad 2. [C] Confidencialidad 3. [D] Disponibilidad
Descripción: Equivocaciones de las personas cuando usan los servicios, datos, etc.	

E.2 Errores del administrador

Tipos de Activos	Dimensiones
[D] Datos / Información [Keys] Claves Criptográficas [S] Servicios [Media] Soportes de Información	1. [I] Integridad 2. [C] Confidencialidad 3. [D] Disponibilidad
Descripción: Equivocaciones de personas con responsabilidades de instalación y operación.	

E.3 Errores de monitorización (log)

Tipos de Activos	Dimensiones
[D.log] Registros de Actividad	1. [I] Integridad (Trazabilidad)
Descripción: Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, etc.	

E.4 Errores de configuración

Tipos de Activos	Dimensiones
[D.conf] Datos de Configuración	1. [I] Integridad
Descripción: Introducción de datos de configuración erróneos: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	

E.5 Deficiencias en la organización

Tipos de Activos	Dimensiones
[P] Personal	1. [D] Disponibilidad
Descripción: Acciones descoordinadas, errores por omisión, etc.	

E.6 Difusión de software dañino

Tipos de Activos	Dimensiones
[SW] Aplicaciones (software)	[D] Disponibilidad [I] Integridad [C] Confidencialidad
Descripción: Propagación inocente de virus, espías (spyware), gusanos, troyanos, etc.	

E.7 Errores de re-encaminamiento

Tipos de Activos	Dimensiones
[S] Servicios [SW] Aplicaciones (software) [COM] Redes de Comunicaciones	[C] Confidencialidad
Descripción: Envío de información a través de un sistema o red, accidentalmente que lleve la información a donde o por donde no es debido.	

E.8 Escapes de información

Tipos de Activos	Dimensiones
	[C] Confidencialidad
Descripción: La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea afectada.	

E.9 Alteración accidental de la información

Tipos de Activos	Dimensiones
[D] Datos / Información [Keys] Claves Criptográficas [S] Servicios [Media] Soportes de Información [SW] Aplicaciones (software) [COM] Redes de Comunicaciones [L] Instalaciones	1. [I] Integridad
Descripción: Sólo se identifica sobre datos en general, cuando está en algún soporte informático hay amenazas específicas.	

E.10 Destrucción de información

Tipos de Activos	Dimensiones
[D] Datos / Información [Keys] Claves Criptográficas [S] Servicios [Media] Soportes de Información [SW] Aplicaciones (software) [COM] Redes de Comunicaciones [L] Instalaciones	1. [D] Disponibilidad
Descripción: Pérdida accidental de información.	

E.11 Fugas de información

Tipos de Activos	Dimensiones
D] Datos / Información [Keys] Claves Criptográficas [S] Servicios [Media] Soportes de Información [SW] Aplicaciones (software) [COM] Redes de Comunicaciones [L] Instalaciones	1. [C] Confidencialidad
Descripción: Revelación por indiscreción.	

E.12 Vulnerabilidades de los programas (software)

Tipos de Activos	Dimensiones
[SW] Aplicaciones (software)	1. [I] Integridad 2. [D] Disponibilidad 3. [C] Confidencialidad
Descripción: Defectos en código que dan pie a una operación defectuosa sin intervención del usuario, con consecuencias en la integridad de datos.	

E.13 Errores de mantenimiento / Actualización de programas (software)

Tipos de Activos	Dimensiones
[SW] Aplicaciones (software)	1. [I] Integridad 2. [D] Disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización del código que permite que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	

E.14 Errores de mantenimiento / Actualización de equipos (hardware)

Tipos de Activos	Dimensiones
[HW] Equipo Informático [Media] Soportes de Información [AUX] Equipamiento Auxiliar	1. [D] Disponibilidad
Descripción: Defectos en la actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	

E.15 Caída del sistema por agotamiento de recursos

Tipos de Activos	Dimensiones
[S] Servicios [HW] Equipo Informático [COM] Redes de Comunicaciones	1. [D] Disponibilidad
Descripción: Carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	

E.16 Pérdida de equipos

Tipos de Activos	Dimensiones
[HW] Equipo Informático [Media] Soportes de Información [AUX] Equipamiento Auxiliar	1. [D] Disponibilidad
Descripción: Provoca la carencia de un medio para prestar los servicios, es decir una	

indisponibilidad.

E.17 Indisponibilidad del personal

Tipos de Activos	Dimensiones
[P] Personal Interno	1. [D] Disponibilidad
Descripción: Ausencia del puesto de trabajo: enfermedad, alteraciones del orden público.	

Ataques intencionales (A)

Fallos deliberados causados por las personas.

A.1 Manipulación de los registros de actividad (log)

Tipos de Activos	Dimensiones
[D.log] Registros de Actividad	1. [I] Integridad (Trazabilidad)

A.2 Manipulación de la configuración

Tipos de Activos	Dimensiones
[D.log] Registros de Actividad	1. [I] Integridad 2. [C] Confidencialidad 3. [A] Autenticidad
Descripción: Todos los activos dependen de su configuración: privilegios de acceso, registro de actividad, encaminamiento, etc.	

A.3 Suplantación de la identidad del usuario

Tipos de Activos	Dimensiones
D] Datos / Información [S] Servicios [SW] Aplicaciones (software) [COM] Redes de Comunicaciones	1. [C] Confidencialidad 2. [A] Autenticidad 3. [I] Integridad
Descripción: Atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para fines propios.	

A.4 Abuso de privilegios de acceso

Tipos de Activos	Dimensiones
D] Datos / Información [Keys] Claves Criptográficas [S] Servicios [SW] Aplicaciones (software) [HW] Equipo Informático	1. [C] Confidencialidad 2. [I] Integridad 3. [D] Disponibilidad

[COM] Redes de Comunicaciones	
Descripción: Un usuario abusa de su nivel de privilegio para realizar tareas que no son de su correspondencia.	

A.5 Uso no previsto

Tipos de Activos	Dimensiones
[S] Servicios [SW] Aplicaciones (software) [HW] Equipo Informático [COM] Redes de Comunicaciones [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [D] Disponibilidad 2. [C] Confidencialidad 3. [I] Integridad
Descripción: Utilización de los recursos del sistema para fines no previstos, juegos, consultas personales en internet, bases de datos o programas personales.	

A.6 Difusión de software dañino

Tipos de Activos	Dimensiones
[SW] Aplicaciones (software)	1. [D] Disponibilidad 2. [I] Integridad 3. [C] Confidencialidad
Descripción: Propagación intencionada de virus, espías (spyware), gusanos, troyanos.	

A.7 Acceso no autorizado

Tipos de Activos	Dimensiones
[D] Datos / Información [Keys] Claves Criptográficas [S] Servicios [SW] Aplicaciones (software) [HW] Equipo Informático [COM] Redes de Comunicaciones [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [C] Confidencialidad 2. [I] Integridad
Descripción: El atacante consigue acceder a los recursos del sistema, típicamente aprovechando un fallo del sistema.	

A.8 Análisis de tráfico

Tipos de Activos	Dimensiones
[COM] Redes de Comunicaciones	1. [C] Confidencialidad 2. [I] Integridad
Descripción: El atacante es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.	

A.9 Repudio

Tipos de Activos	Dimensiones
[S] Servicios [D.log] Registros de Actividad	1. [I] Integridad (trazabilidad)
Descripción: Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.	

A.10 Interceptación de información

Tipos de Activos	Dimensiones
[COM] Redes de Comunicaciones	1. [C] Confidencialidad
Descripción: El atacante obtiene acceso a información que no le corresponde, sin que la información se vea afectada.	

A.11 Modificación deliberada de la información

Tipos de Activos	Dimensiones
[D] Datos / Información [Keys] Claves Criptográficas [S] Servicios [SW] Aplicaciones (software) [COM] Redes de Comunicaciones [Media] Soportes de Información [L] Instalaciones	1. [I] Integridad
Descripción: Alteración intencional de la información para obtener algún beneficio o causar un perjuicio.	

A.12 Destrucción de información

Tipos de Activos	Dimensiones
[D] Datos / Información [Keys] Claves Criptográficas [S] Servicios [SW] Aplicaciones (software) [Media] Soportes de Información [L] Instalaciones	1. [D] Disponibilidad

Descripción: Eliminación intencional de información para obtener algún beneficio o causar un perjuicio.

A.13 Divulgación de información

Tipos de Activos	Dimensiones
[D] Datos / Información [Keys] Claves Criptográficas [S] Servicios [SW] Aplicaciones (software) [COM] Redes de Comunicaciones [Media] Soportes de Información [L] Instalaciones	1. [C] Confidencialidad

A.14 Manipulación de programas

Tipos de Activos	Dimensiones
[SW] Aplicaciones (software)	1. [C] Confidencialidad 2. [I] Integridad 3. [D] Disponibilidad
Descripción: Alteración intencional del funcionamiento de los programas.	

A.15 Manipulación de los equipos

Tipos de Activos	Dimensiones
[HW] Equipo Informático [Media] Soportes de Información [AUX] Equipamiento Auxiliar	1. [C] Confidencialidad 2. [D] Disponibilidad

A.16 Denegación de servicio

Tipos de Activos	Dimensiones
[S] Servicios [SW] Aplicaciones (software) [COM] Redes de Comunicaciones	1. [D] Disponibilidad
Descripción: La carencia de recursos provoca la caída del sistema cuando la carga de trabajo es desmesurada.	

A.17 Robo

Tipos de Activos	Dimensiones
[HW] Equipo Informático [Media] Soportes de Información	1. [D] Disponibilidad 2. [C] Confidencialidad

[AUX] Equipamiento Auxiliar	
Descripción: Sustracción de equipamiento provoca la carencia de un medio para prestar los servicios, es decir una indisponibilidad.	

A.18 Ataque destructivo

Tipos de Activos	Dimensiones
[HW] Equipo Informático [Media] Soportes de Información [AUX] Equipamiento Auxiliar [L] Instalaciones	1. [D] Disponibilidad
Descripción: Vandalismo, terrorismo, acción militar.	

A.19 Indisponibilidad del personal

Tipos de Activos	Dimensiones
[P] Personal Interno	1. [D] Disponibilidad
Descripción: Ausencia deliberada del puesto de trabajo: huelgas, absentismo laboral, bloqueos de los accesos.	

A.20 Ingeniería social

Tipos de Activos	Dimensiones
[P] Personal Interno	1. [C] Confidencialidad 2. [I] Integridad 3. [D] Disponibilidad
Descripción: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	

Anexo 4: Encuesta

ENCUESTA GRP Nº 01

Esta encuesta se aplica con el fin de determinar el nivel de disponibilidad, confidencialidad e integridad de datos y la percepción de los colaboradores sobre el nivel de seguridad de la información existente.

Indicaciones. Lea comprensivamente las preguntas y responda sinceramente marcando con una "X" dentro del paréntesis en una sola alternativa.

Área a la que pertenece: _____

1. ¿Su computador recibe mantenimiento de forma periódica?
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

2. ¿Cuándo se daña su computador que tiempo demoran en arreglarlo?

   Una Hora ☐ Un día ☐

   Dos Horas ☐ Otros ☐

3. ¿Existe algún periodo de tiempo para el cambio o renovación de computadoras?
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

4. ¿Usted apaga su computador cuando se va almorzar?
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

5. ¿Usted guarda la información o la actividad que está realizando cuando sale de su computador?
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

6. ¿Usa nombres, apellidos, fechas de cumpleaños o fechas importantes para la combinación de sus contraseñas?
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

7. ¿Con qué frecuencia cambia su contraseña?
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

8. Usted tiene acceso a internet
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

9. ¿Tiene alguna restricción para ingresar a páginas web?
   SI ( ) NO ( )

10. ¿Posee antivirus su computador?

SI ☐ NO ☐ Esta actualizado: SI ☐ NO ☐

11. ¿Logra identificar con facilidad las extensiones de sus archivos (.exe .jpg .pdf .rar .docx)?
Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

12. ¿Se realizan copias de seguridad de su información?

NUNCA ☐ MENSUAL ☐

SEMANAL ☐ UNA VEZ A AÑO ☐

13. ¿Lleva archivos digitales de su hogar a su trabajo?
Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

14. ¿Ingresa su computadora personal a la institución?
Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

15. ¿Qué sistema gubernamental usa con mayor frecuencia?, valorarlos por dependencia de uso (primero, segundo, tercero u otros si hubieran).

SIGEA ( ) _____ ( )
SIAF ( ) _____ ( )
SIGA ( )
CPRESU ( )
Portal electrónico ( )

16. ¿El equipo informático asignado es obsoleto?

SI ( ) NO ( )

Especifique cual, Monitor ( ) Teclado ( ) Mouse ( )

17. ¿Su equipo cuenta con un equipo UPS o sistema de alimentación ininterrumpida?

SI ( ) NO ( )

18. ¿Actualmente tiene problemas con alguno de estos equipos de comunicación?

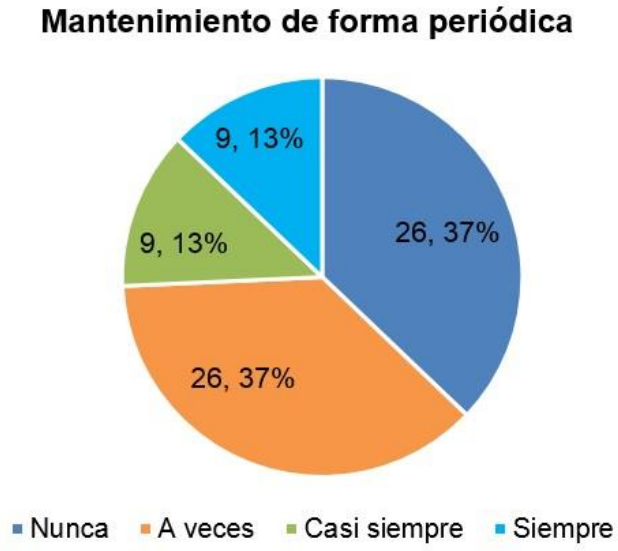
Cable de red ( ) Switch ( ) Otros _____

19. Su oficina se ha visto afectada por alguna de las siguientes amenazas:

FUEGO	☐	TEMBLORES	☐
DAÑOS POR AGUA	☐	CALOR EXTREMO	☐
LLUVIAS	☐		

Anexo 5: Resultados de la encuesta

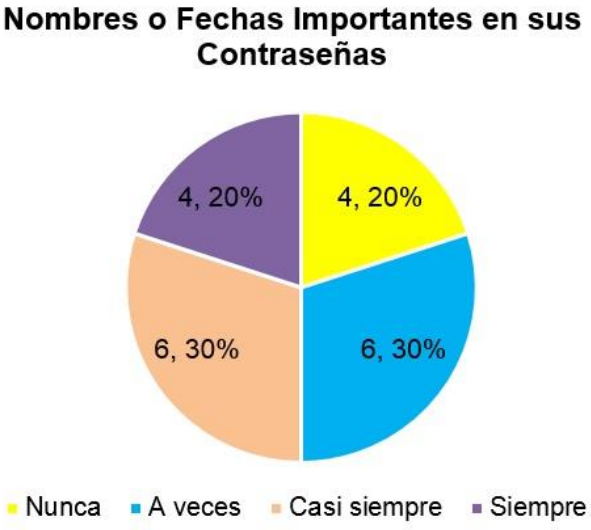
Pregunta 01: ¿Su computador recibe mantenimiento de forma periódica?



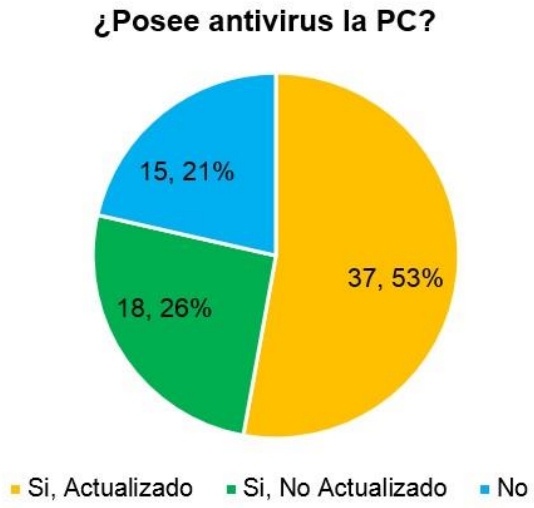
Pregunta 02: ¿Cuándo se daña su computador que tiempo demoran en arreglarlo?

Pregunta 03: ¿Existe algún periodo de tiempo para el cambio o renovación de computadoras?

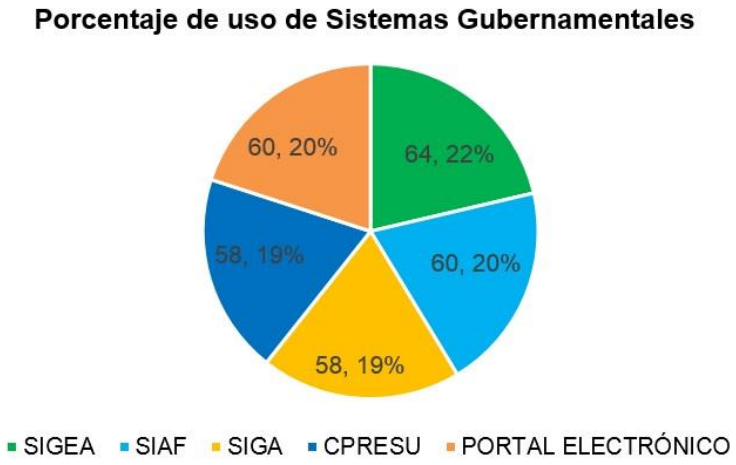
Pregunta 06: ¿Usa nombres, apellidos, fechas de cumpleaños o fechas importantes para la combinación de sus contraseñas?



Pregunta 10: ¿Posee antivirus su computador?



Pregunta 15: ¿Qué sistema gubernamental usa con mayor frecuencia?



Pregunta 19: ¿Su oficina se ha visto afectada por alguna de las siguientes amenazas?

Anexo 6: Desarrollo del análisis de riesgo

Anexo 6.1: Identificación de activos

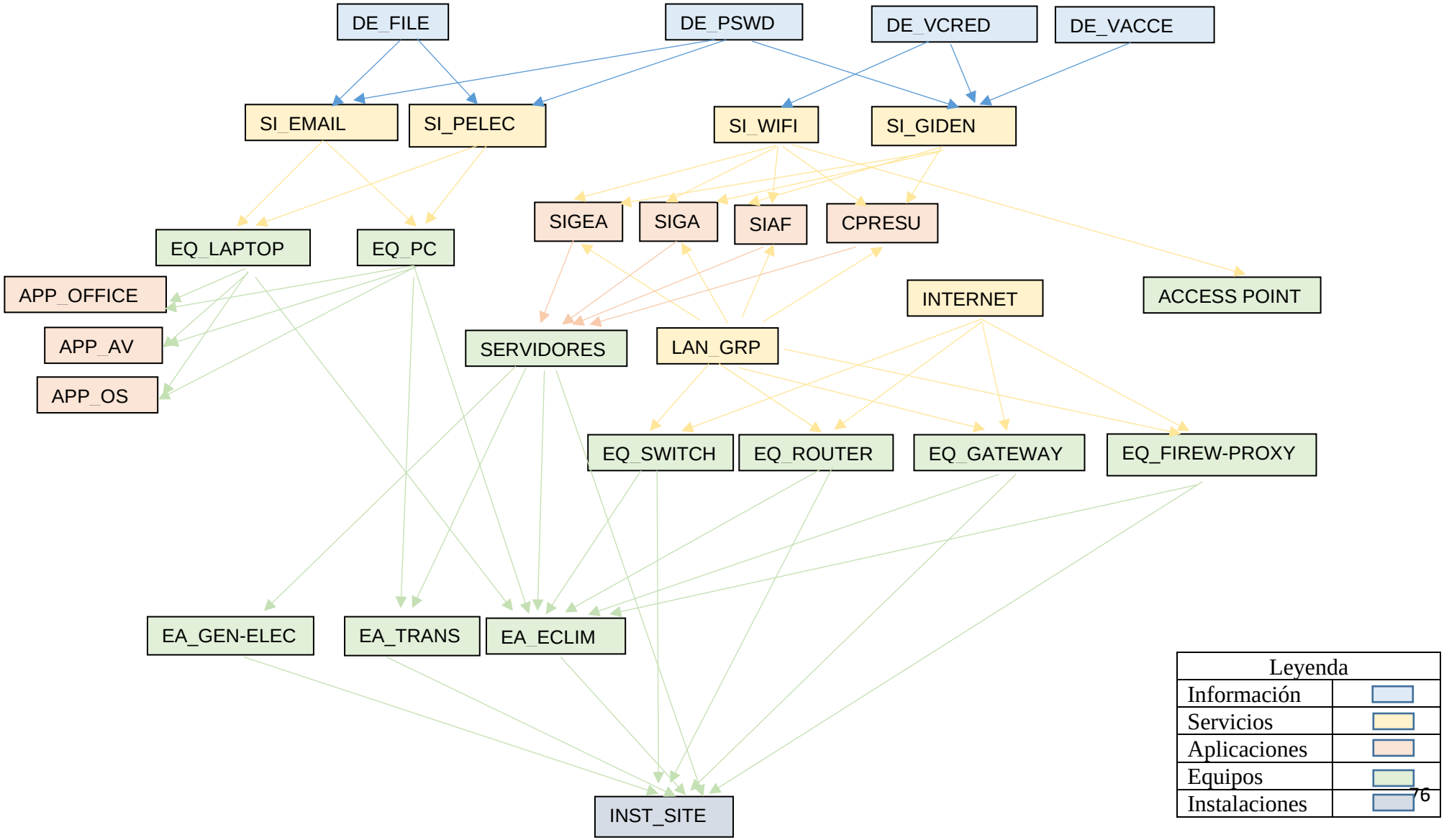
	Activos Esenciales				
	Servicios Esenciales				
N°	Código	Nombre	Descripción	Contenido	Propietario
1	SE_SIGEA	SIGEA	Sistema de Gestión Documentaria	Datos de gestión que permite el seguimiento de los documentos	Henry Nunura
2	SE_SIAF	SIAF	Sistema de Administración Financiera	Datos financieros de la organización	Henry Nunura
3	SE_SIGA	SIGA	Sistema de Gestión Administrativa	Datos administrativos de la organización	Henry Nunura
4	SE_CPRESU	CPRESU	Costos y Presupuestos	Datos de costos y presupuestos de los proyectos de la organización	Henry Nunura
5	SE_EADMI	Expedientes Administrativos Físico	Expedientes de procesos administrativos	Almacena temporalmente datos de procesos informáticos	Jefe de Área
6	SE_AINTER	Acceso a Internet	Requerido para la ejecución de sistemas del gob. Mail, etc		Manuel Ramirez
	Datos Esenciales				
	Código	Nombre	Descripción	Contenido	Propietario
7	DE_FILES	Ficheros	Todos los documentos electrónicos	Almacena archivos digitales	Jefe de Área
8	DE_CDATO	Datos de Configuración	Configuración de servidores, directivas	Almacena la configuración de los servidores, directivas	Henry Nunura
9	DE_PSWD	Credenciales	Credenciales de acceso a los sistemas infc	Credenciales de usuario (dominio LANGRP), administrador, soporte	Henry Nunura
10	DE_VCRED	Datos de Validación de Credenciale	Datos de Validación de Credenciales	Datos de Validación de Credenciales	Henry Nunura
11	DE_CACCE	Datos de Control de Acceso	Datos de control de acceso a sistemas informáticos		Henry Nunura
	Servicios Internos				
	Código	Nombre	Descripción	Contenido	Propietario
12	SI_INTER	Acceso a Internet	Servicio que permite la visualización de páginas web y acceso a diversos protocolos		Manuel Ramirez
13	SI_EMAIL	Correo Electrónico	Servicio que permite envíar correos electrónicos		Manuel Ramirez
14	SI_PELEC	Portal Electrónico	Portal web de la organización	Módulo de transparencia	Manuel Ramirez
15	SI_RWIFI	Acceso a Red Inalámbrica	Servicio de internet inalámbrico		Manuel Ramirez
16	SI_GIDEN	Gestión de Identidades	Servicio que permite altas y bajas de usuar	Credenciales de usuarios del dominio LANGRP y regionpiura.gob.pe	Henry Nunura
17	SI_SBIOM	Sistema Biométrico	Sistema que permite el control de acceso c	Datos de entrada y salida de colaboradores	Henry Nunura

	Equipamiento					
	Aplicaciones					
	Código	Nombre	Descripción	Servicio	Propietario	Versiones / OS
18	APP_NAVEG	Navegador Web	Internet Explorer y Google Chrome	Permite la ejecución de los sistemas gubernamentales y mail	Ivan Cherrez	
19	APP_OFFICE	Ofimática	Software para la creación de archivos de texto, calculo y presentaciones	Permite la creación de archivos de texto, calculo y presentaciones	Ivan Cherrez	2007, 2010, 2013
20	APP_ANTIV	Antivirus	Software para el monitoreo de los equipos y de la red	Permite el monitoreo de los equipos y de la red	Ivan Cherrez	2010
21	APP_SOPER	Sistema Operativo	Software que permite el uso de los equipos tecnológicos a través de interfaces gráficas y ejecución de software		Ivan Cherrez	Microsoft Windows, CentOs, XenServer, Ubunto
22	APP_GMVIR	Gestor de Máquinas Virtuales	Vmware vSphere 5 Hypervisor	Permite virtualizar las maquinas virtuales	Manuel Ramirez	Vmware vSphere 5 Hypervisor
23	APP_BACKUP	Sistema de Backup	Servidor que permite programar las copias de seguridad	Permite el respaldo de Información	Manuel Ramirez	
24	APP_SSRED	Servidor de Servicios de Red	Permite administrar los servicios compartidos de red	Servicio virtualizado del File Server	Henry Nunura	
25	APP_SEMAIL	Servidor de Correos	Permite administrar el tráfico de correos corporativos	Servicio virtualizado de correo corporativo	Henry Nunura	
26	APP_SSIGEA	Servidor Virtualizado SIGEA	Permite administrar el SIGEA	Servicio virtualizado del Sistema de Gestión Administrativa	Henry Nunura	
27	APP_SDOMI	Servidor Virtualizado de Dominio	Permite administrar el Active Directory	Servicio virtualizado del Windows Server 2008 R2	Henry Nunura	
28	APP_SSIAF	Servidor Virtualizado SIAF	Permite administrar el SIAF	Servicio virtualizado del Sistema de Administracion Financiera	Henry Nunura	
29	APP_SCPRESU	Servidor Virtualizado CPRESU	Permite administrar el CPRESU	Servicio virtualizado del Sistema de Costos y Presupuestos	Henry Nunura	
30	APP_SAWEB	Servidor de Aplicaciones Web	Permite administrar las aplicaciones web	Servicio virualizado que permite la administracion de app web	Henry Nunura	

	Equipos							
	Código	Nombre	Descripción	Servicio	Propietario	OS	Características	Cant
31	EQ_SMAIL	IBM SYSTEM-X3400M / Servidor de Correos	Equipo con maquina Virtual de Correos Electrónicos	Email Institucional	Manuel Ramirez	CENTOS 6.5	IBM Intel(R) Xeon(R) CPU	1
32	EQ_SSRED	DELL POWEREDGE R720 / Servicios de Red	Equipo con 7 maquinas Virtuales para Servicios de Red	Servicios de Red	Manuel Ramirez	XenServer 6.1	DELL PowerEdge R720	1
33	EQ_SSICO	DELL POWEREDGE R420 / SIGEA y Dominio	Equipo con 2 maquinas virtuales para SIGEA y controlador de dominio	SIGEA y Controlador de Dominio	Manuel Ramirez	XenServer 6.2	DELL PowerEdge R420	1
34	EQ_SUEIN	DELL POWEREDGE R200 / Unid Ejecutoras e intranet	Equipo con 2 maquinas virtuales para unidades ejecutoras e intranet	Unidades Ejecutoras e Intranet	Manuel Ramirez	Ubuntu 12.04.1 LTS	DELL PowerEdge R200	1
35	EQ_SIACPR	HP SYSTEM 3200 / SIAF y CPRESU	Equipo medio con disco local	SIAF y CPRESU	Manuel Ramirez	Windows Server 2012	HP SYSTEM 3200	1
36	EQ_SVARI	IBM SYSTEM-X3500 / Servidor Varios	Equipo medio con disco local	Agente AV, cheques, softfree. SIMI, anteriores PCUW2000, patrimonio, licencias ACAD, guias, control	Manuel Ramirez	Windows Server 2003	IBM SYSTEM-X3500	1
37	EQ_SANTIV	HP COMPAQ 8200 / Antivirus	Equipo medio con disco local	Antivirus Kaspersky Lab 10	Manuel Ramirez	Windows Server 2012	HP Compaq 8200 Elite Small Form Factor	1
38	EQ_APWEB	IBM SYSTEM-X3500 / Servidor de App Web	Equipo medio con disco local	Aplicaciones Web	Manuel Ramirez	Ubuntu 12.04.1 LTS	IBM SYSTEM-3500 Intel® Xeon® CPU E5335 @ 2.00GHz QUADCORE	1
39	EQ_SMAVIR	DELL PowerEdge 2900 / 3 Máquinas Virtuales	Contiene 3 maquinas virtuales	Contiene 3 maquinas virtuales	Manuel Ramirez	Vmware vSphere 5 Hypervisor	DELL PowerEdge 2900 Intel® Xeon® CPU X5470 @ 3.33GHz 4CPUs	1
40	EQ_LAPTOP	Laptop	Laptop para usuarios	Automatización de procesos	GRP	Vista Home Pro Wind 7, 8.1		35
41	EQ_DESKT	Computadores de Escritorio	PC para usuarios	Automatización de procesos	GRP	Wind XP, 7, 8.1		369
42	EQ_PRINT	Medios de Impresión	Impresoras, Escaner, Multifuncionales	Impresión, copias y escaner	GRP			86
43	EQ_SWITC	Switch	Equipo que permite la comunicación en la red local	Comunicación de equipos en la red LAN	Manuel Ramirez		Cisco 2960X, 3750X - 3COM	15
44	EQ_APOIN	Access Point	Equipos que envían y permiten la conexión WIFI	Acceso Inalámbrico	Manuel Ramirez			3
45	EQ_ROUTE	Router	Equipo que permite la conexión de los equipos a Internet	Ruteador de Red	Manuel Ramirez		Cisco 2900 SERIES	1
46	EQ_GATEW	Gateway	Equipo para interconectar redes, equipo autónomo	Interconexión de redes	Manuel Ramirez		FORTINET, FORTIGATE 200D	2
47	EQ_FIRPR	Firewall / Proxy	Equipo que permite o bloquea las conecciones entrantes a la red	Protección de tráfico datos	Manuel Ramirez		FORTINET, FORTIGATE 200D	1
48	EQ_MBACK	Modem Resplado de Línea de Cobre	Equipo autónomo de respaldo de internet	Respaldo de internet	Manuel Ramirez			1
49	EQ_RBACK	Router Respaldo de Línea de Internet	Equipo autónomo de respaldo de internet	Respaldo de internet	Manuel Ramirez		Cisco 1905	1

	Comunicaciones					
	Código	**Nombre**	**Descripción**	**Servicio**	**Propietario**	**Cantidad**
42	COM_WIFI	WIFI	Acces Point	Red Inalámbrica	Manuel Ramirez	7
43	COM_RLAN	Red de Área Local	Concentrador con n puertos	Red de Área Local	Manuel Ramirez	
44	COM_INTER	Internet			Manuel Ramirez	
	Elementos Auxiliares					
	Código	**Nombre**	**Descripción**	**Servicio**	**Propietario**	**Cantidad**
45	EA_UPS	Sistema de alimentación ininterrumpi	Equipo de protección ante bajas y altas del fluido eléctrico		Manuel Ramirez	8
46	EA_GELEC	Generadores Eléctricos	Generadores Eléctricos	Generador eléctrico en caso de corte de fluido eléctric	Manuel Ramirez	1
47	EA_TAILA	Transformador de Aislamiento KVA	Transformador de Aislamiento KVA	Transformador de aislamiento eléctrico	Rivas	2
48	EA_CLIMA	Equipos de Climatización	Climatización: aire acondicionado, ventiladore	Climatización	GRP	
50	EA_MOBIL	Mobiliario	Armarios, mesas, sillas, rack	Soporte de equipos	GRP	
	Soporte de Información					
	Código	**Nombre**	**Descripción**	**Servicio**	**Propietario**	
51	SI_DDURO	Disco Duro	Disco con una gran capacidad de almacenamiento de datos informáticos		GRP	
52	SI_ALRED	Almacenamiento en Red	Almacenamiento en Red	Permite almacenar datos en red, Write & Read	Manuel Ramirez	
53	SI_CDDVD	CD-ROM & DVD	Sistema Operativo, driver, data		Ivan Cherrez	
54	SI_USB	USB	Medio de transferencia de archivos móvil		USUARIO	
	Instalaciones					
	Código	**Nombre**	**Descripción**			
55	INST_SITE	Recinto	Local Propio			
56	INST_SITEBK	Instalaciones de respaldo in Site	In site, hosting web			
	Personas					
	Código	**Descripción**	**Nombre**			
57	ADM_Sis	Administrador de Sistemas	Henry Nunura			
58	ADM_Com	Administrador de Comunicaciones	Manuel Ramirez			
59	ADM_BD	Administrador de Base de Datos	Henry Nunura			
60	ADM_Sec	Administrador de Seguridad	Henry Nunura - Manuel Ramirez			
61	Prov	Proveedores	Claro, Movistar			

Anexo 6.2: Dependencia de activos



Anexo 6.3: Valoración de activos

Valor		Criterio
5	Extremo	Daño extremadamente grave
4	Muy Alto	Daño muy grave
3	Alto	Daño grave
2	Medio	Daño importante
1	Bajo	Daño menor
0	Despreciable	Irrelevante a efecto de prácticas

N°	Código	Activos	Dimensiones				
		Activos Esenciales	[D]	[I]	[C]	[A]	[T]
		Servicios Esenciales					
1	SE_SIGEA	SIGEA	4	4	4	-	3
2	SE_SIAF	SIAF	4	4	4	-	3
3	SE_SIGA	SIGA	4	4	4	-	3
4	SE_CPRESU	CPRESU	3	3	4	-	3
5	SE_EADMI	Expedientes Administrativos Físicos	4	4	4	-	3
6	SE_AINTER	Acceso a Internet	5	-	-	-	-
		Datos Esenciales					
7	DE_FILES	Ficheros	4	4	4	-	1
8	DE_CDATO	Datos de Configuración	3	3	4	-	-
9	DE_PSWD	Credenciales	1	1	2	-	-
10	DE_VCRED	Datos de Validación de Credenciales	3	3	3	-	-
11	DE_CACCE	Datos de Control de Acceso	3	3	2	-	-
		Servicios Internos					
12	SI_INTER	Correo Electrónico	2	-	-	2	2
13	SI_EMAIL	Portal Electrónico	3	4	-	-	2
15	SI_PELEC	Gestión de Identidades	2	-	-	-	2
16	SI_RWIFI	Acceso a Red Inalámbrica	4	-	-	-	-
		Equipamiento					
		Aplicaciones					
17	APP_NAVEG	Navegador Web Google Chrome e IE	2	-	-	-	-
18	APP_OFFICE	Ofimática	3	2	-	-	-
19	APP_ANTIV	Antivirus	3	-	-	-	-
20	APP_SOPER	Sistema Operativo	5	3	3	-	-
21	APP_GMVIR	Gestor de Máquinas Virtuales	4	-	-	-	-
22	APP_BACKUP	Sistema de Backup	4	-	-	-	-
23	APP_SSRED	Servidor de Servicios de Red	4	4	4	4	3
24	APP_SEMAIL	Servidor de Correos	4	4	4	4	4
25	APP_SSIGEA	Servidor Virtualizado SIGEA	4	4	4	4	3
26	APP_SDOMI	Servidor Virtualizado de Dominio	4	4	4	4	3
27	APP_SSIAF	Servidor Virtualizado SIAF	4	4	4	4	3
28	APP_SCPRESU	Servidor Virtualizado CPRESU	4	4	4	4	3
29	APP_SAWEB	Servidor de Aplicaciones Web	4	4	4	4	3

		Equipos					
		Servidor					
30	EQ_SMAIL	IBM SYSTEM-X3400M / Servidor de Correos	3	3	3	-	-
31	EQ_SSRED	DELL POWEREDGE R720 / Servicios de Red	4	4	3	-	-
32	EQ_SSICO	DELL POWEREDGE R420 / SIGEA y Controlador de Dom	5	5	3	-	-
33	EQ_SUEIN	DELL POWEREDGE R200 / Unidades Ejecutoras e intra	5	5	3	-	-
34	EQ_SIACPR	HP SYSTEM 3200 / SIAF y CPRESU	5	5	3	-	-
35	EQ_SVARI	IBM SYSTEM-X3500 / Servidor Varios	1	1	1	-	-
36	EQ_SANTIV	HP COMPAQ 8200 / Antivirus	3	-	-	-	-
37	EQ_APWEB	IBM SYSTEM-X3500 / Servidor de Aplicaciones Web	3	3	3	-	-
38	EQ_SMAVIR	DELL PowerEdge 2900 / 3 Máquinas Virtuales	2	2	-	-	-
39	EQ_LAPTOP	Laptop	4	3	3	-	1
40	EQ_DESKT	Computadores de Escritorio	4	3	3	-	1
41	EQ_PRINT	Medios de Impresión	3	-	-	-	-
42	EQ_SWITC	Switch	4	-	-	-	-
43	EQ_APOIN	Access Point	4	-	-	-	-
44	EQ_ROUTE	Router	3	-	-	-	-
45	EQ_GATEW	Gateway	4	-	-	-	-
46	EQ_FIRPR	Firewall / Proxy	4	-	-	-	-
47	EQ_MBACK	Modem Respaldo de Línea de Cobre	3	-	-	-	-
48	EQ_RBACK	Router Respaldo de Línea de Internet	3	-	-	-	-
		Comunicaciones					
41	COM_WIFI	WIFI	4	-	-	-	-
42	COM_RLAN	Red de Área Local	4	-	-	-	-
43	COM_INTER	Internet	5	-	-	-	-
		Elementos Auxiliares					
44	EA_UPS	Sistema de Alimentación Ininterrumpida	2	-	-	-	-
45	EA_GELEC	Generadores Eléctricos	2	-	-	-	-
46	EA_TAILA	Transformador de Aislamiento KVA	2	-	-	-	-
47	EA_CLIMA	Equipos de Climatización	3	-	-	-	-
49	EA_MOBIL	Mobiliario	1	-	-	-	-
		Soporte de Información					
50	SI_DDURO	Disco Duro	3	3	3	-	-
51	SI_ALRED	Almacenamiento en Red	1	-	-	-	-
52	SI_CDDVD	CD-ROM & DVD	1	-	-	-	-
53	SI_USB	USB	1	-	-	-	-
		Instalaciones					
54	INST_SITE	Recinto	4	-	-	-	-
55	INST_SITEBK	Instalaciones de respaldo in Site	4	-	-	-	-
		Personal					
56	ADM_Sis	Administrador de Sistemas	3				
57	ADM_Com	Administrador de Comunicaciones	3				
58	ADM_BD	Administrador de Base de Datos	3				
59	ADM_Sec	Administrador de Seguridad	3				
60	PROVE	Proveedores	0				

Anexo 6.4: Identificación de amenazas

N°	Activos Activos Esenciales Servicios Esenciales	Amenazas	Dimensión
1	SIGEA SIAF SIGA CPRESU	I.3. Avería de origen físico o lógico	D
2		E.1 Errores de los usuarios	I, C, D
3		E.11 Vulnerabilidades de los programas	I, D, C
4		E.12 Errores de mantenimiento o actualizaciones de programa	I, D
5		A.4 Uso no previsto	D, C, I
6		A.6 Acceso no autorizado	C, I
7		E.3 Errores de monitorización (actividad, log)	I
8	Expedientes Administrativos Físicos	E.1 Errores de los usuarios	I, C, D
9		I.1 Fuego	D
10		A.11 Destrucción intencional de la información	D
11		A.14 Robo	D, C
12		A.10 Modificación deliberada de la información	I
13	Acceso a Internet	I.6 Fallos de servicios de comunicaciones	D
14		A.5 Difusión de software dañino	D, I, C
15		A.8 Repudio	I (T)
16		A.4 Uso no previsto	D, C, I
	Datos Esenciales		
17	Ficheros	E.1 Errores de los usuarios	I, C, D
18		A.4 Uso no previsto	D, C, I
19		A.6 Acceso no autorizado	C, I
20		A.19 Virus Informático	D,I,C
21		A.14 Robo de Datos	D, C
22		A.11 Destrucción intencional de la información	D
23		A.10 Modificación deliberada de la información	I
24		E.8 Alteración accidental de la información	I
25	Datos de Configuración	E.2 Errores del administrador	D,I,C
26		E.8 Alteración accidental de la información	I
27		A.1 Manipulación de la configuración	I, C, D
28		A.6 Acceso no autorizado	C, I
29		E.4 Errores de configuración	I
30	Credenciales	A.17 Ingeniería social	C, I, D
31		E.2 Errores del administrador	D,I,C
32	Datos de Validación de Credenciales - Datos de Control de Acceso	E.2 Errores del administrador	D,I,C
33		E.8 Alteración accidental de la información	I
34		A.6 Acceso no autorizado	C, I
35		E.4 Errores de configuración	I
	Servicios Internos		
36	Correo Electrónico	E.1 Errores de los usuarios	I, C, D
37		E.10 Fuga de información	C
38		A.8 Repudio	I (T)
39		A.4 Uso no previsto	D, C, I
40	Portal Electrónico	E.1 Errores de los usuarios	I, C, D
41		A.8 Repudio	I (T)
42		E.8 Alteración accidental de la información	I
43	Acceso a Red Inalámbrica	E.2 Errores del administrador	D,I,C
44		A.4 Uso no previsto	D, C, I
45		A.2 Suplantación de la identidad del usuario	C, A, I
46	Gestión de Identidades	E.2 Errores del administrador	D,I,C

	Equipamiento		
	Aplicaciones		
47	Navegador Web	E.1 Errores de los usuarios	I, C, D
48		A.4 Uso no previsto	D, C, I
49		A.12 Manipulación intencional de programas	C, I, D
50		E.5 Difusión de software dañino	D,I,C
51	Ofimática	E.1 Errores de los usuarios	I, C, D
52		E.12 Errores de mantenimiento o actualizaciones de programa	I, D
53		A.4 Uso no previsto	D, C, I
54		E.11 Vulnerabilidades de los programas	I, D, C
55	Antivirus	E.11 Vulnerabilidades de los programas	I, D, C
56		E.12 Errores de mantenimiento o actualizaciones de programa	I, D
57	Sistema Operativo	I.3. Avería de origen físico o lógico	D
58		E.5 Difusión de software dañino	D,I,C
59		E.11 Vulnerabilidades de los programas	I, D, C
60		A.20 Ataques Informáticos	D,I,C
61		A.19 Virus Informático	D,I,C
62		E.12 Errores de mantenimiento o actualizaciones de programa	I, D
63		A.4 Uso no previsto	D, C, I
64		E.1 Errores de los usuarios	I, C, D
65	Gestor de Máquinas Virtuales	E.2 Errores del administrador	D,I,C
66		E.11 Vulnerabilidades de los programas	I, D, C
67		E.12 Errores de mantenimiento o actualizaciones de programa	I, D
68	Sistema de Backup	E.2 Errores del administrador	D,I,C
69	Servidor de Servicios de Red	A.20 Ataques Informáticos	D,I,C
70	Servidor de Correos	A.13 Denegación de servicio (carga desmesurada de trabajo)	D
71	Servidor Virtualizado SIGEA	A.2 Suplantación de la identidad del usuario	C, A, I
72	Servidor Virtualizado Controlador de D	E.6 Errores de reencaminamiento	C
73	Servidor Virtualizado SIAF	E.11 Vulnerabilidades de los programas	I, D, C
74	Servidor Virtualizado CPRESU	A.19 Virus Informático	D,I,C
75	Servidor de Aplicaciones Web	E.2 Errores del administrador	D,I,C
76		E.12 Errores de mantenimiento o actualizaciones de programa	I, D
77		A.6 Acceso no autorizado	C, I
78	**Equipos**		
79	DELL POWEREDGE R720 / Servicios de R	I.2 Contaminación Mecánica (polvo, suciedad)	D
80	IBM SYSTEM-X3400M / Servidor de Cor	I.1 Fuego	D
81	DELL POWEREDGE R420 / SIGEA y Contr	N.2 Desastres naturales - Sismos, Terremotos	D
82	DELL POWEREDGE R200 / Unidades Ejec	I.3. Avería de origen físico o lógico	D
83	HP SYSTEM 3200 / SIAF y CPRESU	I.4 Corte del suministro eléctrico	D
84	IBM SYSTEM-X3500 / Servidor Varios	I.5 Condiciones inadecuadas de temperatura o humedad	D
85	HP COMPAQ 8200 / Antivirus	I.8 Degradación de los soportes de almacenamiento de información	D
86	IBM SYSTEM-X3500 / Servidor de Aplica	E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	D
87	DELL PowerEdge 2900 / 3 Máquinas Vir	E.2 Errores del administrador	D,I,C
88		E.9 Destrucción de la información	D
89		A.18 Manipulación del hardware	C,D
90		A.6 Acceso no autorizado	C, I
91		E.3 Errores de monitorización (actividad, log)	I
90	Laptop	E.1 Errores de los usuarios	I, C, D
91		I.2 Contaminación Mecánica (polvo, suciedad)	D
92		E.9 Destrucción de la información	D
93		E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	D
94		E.14 Pérdida de equipos	D, C
95		I.3. Avería de origen físico o lógico	D
96		I.5 Condiciones inadecuadas de temperatura	D
97		I.1 Fuego	D
98		A.20 Ataques Informáticos	D,I,C
99		A.4 Uso no previsto	D, C, I
100		A.6 Acceso no autorizado	C, I
101		A.14 Robo	D, C
102		E.5 Difusión de software dañino	D,I,C

103	Computadores de Escritorio	E.1 Errores de los usuarios	I, C, D
104		E.5 Difusión de software dañino	D,I,C
105		I.2 Contaminación Mecánica (polvo, suciedad)	D
106		E.9 Destrucción de la información	D
107		I.5 Condiciones inadecuadas de temperatura	D
108		I.3. Avería de origen físico o lógico	D
109		A.20 Ataques Informáticos	D,I,C
110		I.1 Fuego	D
111		A.6 Acceso no autorizado	C, I
112		A.4 Uso no previsto	D, C, I
113		E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	D
114	Medios de Impresión	I.7 Interrupción de otros servicios y suministros esenciales	D
115		E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	D
116		A.6 Acceso no autorizado	C, I
117		I.1 Fuego	D
118		I.2 Contaminación Mecánica (polvo, suciedad)	D
119		I.3. Avería de origen físico o lógico	D
120		A.4 Uso no previsto	D, C, I
121		E.1 Errores de los usuarios	I, C, D
122	Switch	I.6 Fallos de servicios de comunicaciones	D
123		E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	D
124		I.2 Contaminación Mecánica (polvo, suciedad)	D
125		I.3. Avería de origen físico o lógico	D
126		E.14 Pérdida de equipos	D, C
127		A.4 Uso no previsto	D, C, I
128		A.14 Robo	D, C
129	Access Point	I.1 Fuego	D
130		I.2 Contaminación Mecánica (polvo, suciedad)	D
131		I.3. Avería de origen físico o lógico	D
132		A.14 Robo	D
133		I.6 Fallos de servicios de comunicaciones	D
134		E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	D
135	Router	I.6 Fallos de servicios de comunicaciones	D
136		I.3. Avería de origen físico o lógico	D
137		I.2 Contaminación Mecánica (polvo, suciedad)	D
138		E.2 Errores del administrador	D,I,C
139		E.14 Pérdida de equipos	D, C
140		A.14 Robo	D, C
141		E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	D
142	Gateway	I.6 Fallos de servicios de comunicaciones	D
143		E.13 Errores de mantenimiento o actualizacion de equipo	D
144	Firewall / Proxy	I.6 Fallos de servicios de comunicaciones	D
145		E.13 Errores de mantenimiento o actualizacion de equipo	D
	Comunicaciones		
146	WIFI	E.2 Errores del administrador	D,I,C
147		A.4 Uso no previsto	D, C, I
148		A.6 Acceso no autorizado	C, I
149		I.6 Fallos de servicios de comunicaciones	D
150		A.7 Análisis de tráfico	C
151		A.9 Interceptación de información (escucha)	C
152		A.2 Suplantación de la identidad del usuario	C, A, I
153	Red de Área Local	E.2 Errores del administrador	D,I,C
154		A.6 Acceso no autorizado	C, I
155		I.6 Fallos de servicios de comunicaciones	D
156		A.9 Interceptación de información (escucha)	C
157		A.7 Análisis de tráfico	C
158		A.4 Uso no previsto	D, C, I
159	Internet	E.2 Errores del administrador	D,I,C
160		I.6 Fallos de servicios de comunicaciones	D
161		A.13 Denegación de servicio (carga desmesurada de trabajo)	D
162		A.4 Uso no previsto	D, C, I

	Elementos Auxiliares		
163	Sistema de Alimentación Ininterrumpi	I.1 Fuego	D
164	Generadores Elétricos	I.3. Avería de origen físico o lógico	D
165	Transformador de Aislamiento KVA	I.4 Corte del suministro eléctrico	D
166		I.2 Contaminación Mecánica (polvo, suciedad)	D
167	Equipos de Climatización	I.5 Condiciones inadecuadas de temperatura	D
168		I.7 Interrupción de otros servicios y suministros esenciales	D
169		E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	D
170		I.1 Fuego	D
171	Mobiliario	A.4 Uso no previsto	D, C, I
172		N.2 Agua	D
	Soporte de Información		
173		I.1 Fuego	D
174		E.14 Pérdida de equipos	D, C
175		I.8 Degradación de los soportes de almacenamiento de información	D
176	Disco Duro	I.2 Contaminación Mecánica (polvo, suciedad)	D
177		A.4 Uso no previsto	D, C, I
178		A.14 Robo	D, C
179		I.3. Avería de origen físico o lógico	D
180		E.2 Errores del administrador	D,I,C
181	Almacenamiento en Red	A.6 Acceso no autorizado	C, I
182		A.4 Uso no previsto	D, C, I
183		I.1 Fuego	D
184	CD-ROM & DVD	I.8 Degradación de los soportes de almacenamiento de información	D
185		A.14 Robo	D, C
186		A.4 Uso no previsto	D, C, I
187		I.3. Avería de origen físico o lógico	D
188		A.4 Uso no previsto	D, C, I
189	USB	A.14 Robo	D, C
190		E.14 Pérdida de equipos	D, C
191		I.8 Degradación de los soportes de almacenamiento de información	D
	Instalaciones		
192		I.1 Fuego	D
193	Recinto	N.1 Daños por agua	D
194		N.3 Calor Extremo	D
195	Instalaciones de respaldo in Site	N.2 Desastres naturales	D
196		A.15 Ataque destructivo (vandalismo, terrorismo)	D
	Personal		
197	Administrador de Sistemas	A.17 Ingeniería social	C, I, D
198	Administrador de Comunicaciones	E.7 Escapes de información	C
199	Administrador de Base de Datos	E.15 Indisponibilidad del personal	D
200	Administrador de Seguridad	A.3 Abuso de privilegios de acceso	C, I, D
201	Usuarios Internos	A.16 Indisponibilidad deliberada de personal (huelgas)	D

Anexo 6.5: Valoración de amenazas

Degradación de Valor			
5	100%	Muy Alta	Casi Seguro
4	80%	Alta	Muy Alto
3	50%	Media	Posible
2	10%	Baja	Poco Probable
2	1%	Muy Baja	Muy Rara
0			

N°	Activos Activos Esenciales Servicios Esenciales	Amenazas	Probabilidad Ocurrencia			[D]	[I]	[C]	[A]	[T]
			S	V	NPO					
1		I.3. Avería de origen físico o lógico	N	3		3	-	-	-	-
2	SIGEA	E.1 Errores de los usuarios	PF	2		1	3	1	-	-
3	SIAF	E.11 Vulnerabilidades de los programas	PF	2	2	3	3	3	-	-
4	SIGA	E.12 Errores de mantenimiento o actualizaciones de programa	N	2		3	4	-	-	-
5	CPRESU	A.4 Uso no previsto	N	2		1	1	1	-	-
6		A.6 Acceso no autorizado	N	3		-	4	5	-	-
7		E.1 Errores de los usuarios	PF	2		3	4	3	-	-
8		A.11 Destrucción intencional de la información	N	3		4	-	-	-	-
9	Expedientes Administrativos Físicos	I.1 Fuego	F	4	3	5	-	-	-	-
10		A.14 Robo	N	3		4	-	3	-	-
11		A.10 Modificación deliberada de la información	N	3		-	5	-	-	-
12		I.6 Fallos de servicios de comunicaciones	F	4		4	-	-	-	-
13		A.13 Denegación de servicio (carga desmesurada de trabajo)	N	3		4	-	-	-	-
14	Acceso a Internet	A.5 Difusión de software dañino	N	2	3	3	1	3	-	-
15		A.8 Repudio	PF	2		-	-	-	-	2
16		A.4 Uso no previsto	N	3		2	0	0	-	-
	Datos Esenciales									
17		E.1 Errores de los usuarios	PF	2		1	4	2	-	-
18		A.4 Uso no previsto	N	3		2	2	2	-	-
19		A.6 Acceso no autorizado	F	4		-	4	4	-	-
20	Ficheros	A.19 Virus Informático	MF	5	3	3	3	3	-	-
21		A.14 Robo de Datos	F	4		3	3	3	-	-
22		A.11 Destrucción intencional de la información	F	4		5	-	-	-	-
23		A.10 Modificación deliberada de la información	N	3		-	5	-	-	-
24		E.8 Alteración accidental de la información	PF	2		-	4	-	-	-
25		E.2 Errores del administrador	N	3		3	3	3	-	-
26		E.8 Alteración accidental de la información	N	3		-	3	-	-	-
27	Datos de Configuración	A.1 Manipulación de la configuración	PF	2	3	2	4	2	-	-
28		A.6 Acceso no autorizado	PF	2		-	5	4	-	-
29		E.4 Errores de configuración	N	3		-	3	-	-	-
30		E.2 Errores del administrador	N	3		3	3	3	-	-
31	Datos de Validación de Credenciales -	E.8 Alteración accidental de la información	N	3	3	-	3	-	-	-
32	Datos de Control de Acceso	A.6 Acceso no autorizado	PF	2		-	4	-	-	-
33		E.4 Errores de configuración	N	3		-	3	-	-	-
	Servicios Internos									
34		E.8 Alteración accidental de la información	PF	2		-	3	-	-	-
35	Portal Electrónico	A.8 Repudio	PF	2	2	-	-	-	-	2
36		E.1 Errores de los usuarios	N	3		2	2	0	-	-
37		E.2 Errores del administrador	N	3		3	1	3	-	-
38	Acceso a Red Inalámbrica	A.4 Uso no previsto	F	4	3	2	1	1	-	-
39		A.2 Suplantación de la identidad del usuario	N	3		-	3	3	3	-

	Equipamiento									
	Aplicaciones									
40	Ofimática	E.1 Errores de los usuarios	N	3	4	3	2	0	-	-
41		E.12 Errores de mantenimiento o actualizaciones de programa	MF	5		3	3	3	-	-
42		A.4 Uso no previsto	F	4		1	1	1	-	-
43		E.11 Vulnerabilidades de los programas	MF	5		4	3	3	-	-
44	Sistema Operativo	I.3. Avería de origen físico o lógico	N	3	4	4	-	-	-	-
45		E.5 Difusión de software dañino	F	4		4	3	2	-	-
46		A.20 Ataques Informáticos	N	3		4	4	4	-	-
47		E.11 Vulnerabilidades de los programas	MF	5		5	4	4	-	-
48		A.19 Virus Informático	MF	5		4	3	3	-	-
49		E.12 Errores de mantenimieto o actualizaciones de programa	MF	5		5	4	-	-	-
50		A.4 Uso no previsto	F	4		4	3	3	-	-
51		E.1 Errores de los usuarios	F	4		4	3	3	-	-
52		A.20 Ataques Informáticos	N	3	3	4	4	4	-	-
53	Servidor de Servicios de Red	A.13 Denegación de servicio (carga desmesurada de trabajo)	N	3		5	-	-	-	-
54	Servidor de Correos	A.2 Suplantación de la identidad del usuario	N	3		-	3	3	3	-
55	Servidor Virtualizado SIGEA	E.11 Vulnerabilidades de los programas	PF	2		3	3	3	-	-
56	Servidor Virtualizado Controlador de D	A.19 Virus Informático	PF	2		3	3	3	-	-
57	Servidor Virtualizado SIAF	E.2 Errores del administrador	N	3		3	3	3	-	-
58	Servidor Virtualizado CPRESU	E.12 Errores de mantenimiento o actualizaciones de programa	N	3		3	3	-	-	-
59	Servidor de Aplicaciones Web	A.6 Acceso no autorizado	N	3		-	4	4	-	-
	Equipos									
60		I.2 Contaminación Mecánica (polvo, suciedad)	N	3	3	2	-	-	-	-
61		I.1 Fuego	PF	2		4	-	-	-	-
62		I.3. Avería de origen físico o lógico	F	4		4	-	-	-	-
63	IBM SYSTEM-X3400M / Servidor de Cor	I.4 Corte del suministro eléctrico	N	3		2	-	-	-	-
64	DELL POWEREDGE R720 / Servicios de R	I.5 Condiciones inadecuadas de temperatura o humedad	MF	5		3	-	-	-	-
65	DELL POWEREDGE R420 / SIGEA y Contr	I.8 Degradación de los soportes de almacenamiento de inform	F	4		4	-	-	-	-
66	DELL POWEREDGE R200 / Unidades Ejec	E.13 Errores de mantenimiento o actualizacion de equipo (har	F	4		4	-	-	-	-
67	HP SYSTEM 3200 / SIAF y CPRESU	N.2 Desastres naturales	MPF	1		4	-	-	-	-
68		E.2 Errores del administrador	N	3		3	3	3	-	-
69		E.9 Destrucción de la información	PF	2		4	-	-	-	-
70		A.18 Manipulación del hardware	PF	2		4	-	2	-	-
71		A.6 Acceso no autorizado	PF	2		-	4	2	-	-
72		E.3 Errores de monitorización (actividad, log)	N	3		-	3	-	-	-
73	Laptop	E.1 Errores de los usuarios	F	4	3	2	2	2	-	-
74		I.2 Contaminación Mecánica (polvo, suciedad)	F	4		3	-	-	-	-
75		E.9 Destrucción de la información	N	3		2	-	-	-	-
76		E.13 Errores de mantenimiento o actualizacion de equipo (har	F	4		3	-	-	-	-
77		E.14 Pérdida de equipos	PF	2		-	4	4	-	-
78		I.3. Avería de origen físico o lógico	N	3		3	-	-	-	-
79		I.5 Condiciones inadecuadas de temperatura	F	4		3	-	-	-	-
80		A.20 Ataques Informáticos	N	3		4	4	4	-	-
81		I.1 Fuego	F	4		5	-	-	-	-
82		A.4 Uso no previsto	MF	5		3	3	3	-	-
83		A.6 Acceso no autorizado	PF	2		-	4	4	-	-
84		A.14 Robo	PF	2		5	5	5	-	-
85		E.5 Difusión de software dañino	F	4		3	3	3	-	-
86	Computadores de Escritorio	E.1 Errores de los usuarios	F	4	4	2	2	2	-	-
87		E.5 Difusión de software dañino	F	4		3	3	3	-	-
88		I.2 Contaminación Mecánica (polvo, suciedad)	F	4		3	-	-	-	-
89		E.9 Destrucción de la información	N	3		3	-	-	-	-
90		I.5 Condiciones inadecuadas de temperatura	F	4		3	-	-	-	-
91		I.3. Avería de origen físico o lógico	N	3		4	-	-	-	-
92		A.20 Ataques Informáticos	N	3		4	4	4	-	-
93		I.1 Fuego	MF	5		5	-	-	-	-
94		A.6 Acceso no autorizado	N	3		-	4	4	-	-
95		A.4 Uso no previsto	MF	5		3	3	3	-	-
96		E.13 Errores de mantenimiento o actualizacion de equipo (har	F	4		4	-	-	-	-

97	Medios de Impresión	I.7 Interrupción de otros servicios y suministros esenciales	MF	5	4	3	-	-	-	-
98		E.13 Errores de mantenimiento o actualizacion de equipo (har	MF	5		4	-	-	-	-
99		A.6 Acceso no autorizado	MF	5		-	1	0	-	-
100		I.1 Fuego	N	3		5	-	-	-	-
101		I.2 Contaminación Mecánica (polvo, suciedad)	F	4		2	-	-	-	-
102		I.3. Avería de origen físico o lógico	F	4		4	-	-	-	-
103		A.4 Uso no previsto	F	4		2	0	0	-	-
104		E.1 Errores de los usuarios	F	4		3	1	0	-	-
105	Switch	I.6 Fallos de servicios de comunicaciones	N	3	2	5	-	-	-	-
106		E.13 Errores de mantenimiento o actualizacion de equipo (har	N	3		4	-	-	-	-
107		I.2 Contaminación Mecánica (polvo, suciedad)	F	4		2	-	-	-	-
108		I.3. Avería de origen físico o lógico	N	3		4	-	-	-	-
109		E.14 Pérdida de equipos	MPF	1		5	-	0	-	-
110		A.4 Uso no previsto	PF	2		1	0	0	-	-
111		A.14 Robo	MPF	1		5	-	0	-	-
112	Access Point	I.1 Fuego	N	3	3	5	-	-	-	-
113		I.2 Contaminación Mecánica (polvo, suciedad)	F	4		3	-	-	-	-
114		I.3. Avería de origen físico o lógico	PF	2		3	-	-	-	-
115		A.14 Robo	MPF	1		5	-	-	-	-
116		I.6 Fallos de servicios de comunicaciones	PF	2		3	-	-	-	-
117		E.13 Errores de mantenimiento o actualizacion de equipo (har	N	3		4	-	-	-	-
118	Router	I.6 Fallos de servicios de comunicaciones	N	3	3	5	-	-	-	-
119		I.3. Avería de origen físico o lógico	N	3		4	-	-	-	-
120		I.2 Contaminación Mecánica (polvo, suciedad)	F	4		2	-	-	-	-
121		E.2 Errores del administrador	N	3		2	1	1	-	-
122		E.14 Pérdida de equipos	MPF	1		5	-	0	-	-
123		A.14 Robo	MPF	1		5	-	0	-	-
124		E.13 Errores de mantenimiento o actualizacion de equipo (har	N	3		4	-	-	-	-
	Comunicaciones									
125	WIFI	E.2 Errores del administrador	N	3	3	2	3	3	-	-
126		A.4 Uso no previsto	PF	2		2	1	1	-	-
127		A.6 Acceso no autorizado	N	3		-	3	3	-	-
128		I.6 Fallos de servicios de comunicaciones	N	3		4	-	-	-	-
129		A.7 Análisis de tráfico	F	4		-	-	4	-	-
130		A.9 Interceptación de información (escucha)	N	3		-	-	3	-	-
131		A.2 Suplantación de la identidad del usuario	N	3		-	3	3	3	-
132	Red de Área Local	E.2 Errores del administrador	N	3	3	2	3	3	-	-
133		A.6 Acceso no autorizado	MF	5		-	3	3	-	-
134		I.6 Fallos de servicios de comunicaciones	N	3		4	-	-	-	-
135		A.9 Interceptación de información (escucha)	N	3		-	-	4	-	-
136		A.7 Análisis de tráfico	N	3		-	-	4	-	-
137		A.4 Uso no previsto	PF	2		2	2	1	-	-
138	Internet	E.2 Errores del administrador	PF	2	3	4	2	2	-	-
139		I.6 Fallos de servicios de comunicaciones	F	4		5	-	-	-	-
140		A.13 Denegación de servicio (carga desmesurada de trabajo)	F	4		5	-	-	-	-
141		A.4 Uso no previsto	N	3		1	0	0	-	-
	Elementos Auxiliares									
142	Equipos de Climatización	I.1 Fuego	N	3	3	3	-	-	-	-
143		I.3. Avería de origen físico o lógico	F	4		3	-	-	-	-
144		I.4 Corte del suministro eléctrico	N	3		2	-	-	-	-
145		I.2 Contaminación Mecánica (polvo, suciedad)	F	3		2	-	-	-	-
146		I.7 Interrupción de otros servicios y suministros esenciales	N	3		4	-	-	-	-
147		E.13 Errores de mantenimiento o actualizacion de equipo (har	F	4		3	-	-	-	-
	Soporte de Información									
148	Disco Duro	I.1 Fuego	MPF	1	4	5	-	-	-	-
149		E.14 Pérdida de equipos	F	4		5	-	5	-	-
150		I.8 Degradación de los soportes de almacenamiento de inform	MF	5		4	-	-	-	-
151		I.2 Contaminación Mecánica (polvo, suciedad)	F	4		3	-	-	-	-
152		A.4 Uso no previsto	F	4		2	2	2	-	-
153		A.14 Robo	F	4		5	-	5	-	-
154		I.3. Avería de origen físico o lógico	MF	5		4	-	-	-	-
	Instalaciones									
155		I.1 Fuego	N	3	3	3	-	-	-	-
156	Recinto	N.1 Daños por agua	N	3		3	-	-	-	-
157		N.3 Calor Extremo	F	4		4	-	-	-	-
158	Instalaciones de respaldo	N.2 Desastres naturales	N	3		4	-	-	-	-
159		A.15 Ataque destructivo (vandalismo, terrorismo)	F	4		3	-	-	-	-

Anexo 6.6: Impacto potencial

Valor	Criterio
5	Muy Alto
4	Alto
3	Medio
2	Bajo
1	Muy Bajo
0	Despreciable

N°	Activos Activos Esenciales Servicios Esenciales	[D]	[I]	[C]	[A]	[T]	Me
1	SIGEA	3	3	3	-	-	3
2	SIAF	3	3	3	-	-	3
3	SIGA	3	3	3	-	-	3
4	CPRESU	3	3	3	-	-	3
5	Expedientes Administrativos Físicos	4	4	3	-	-	4
6	Acceso a Internet	4	-	-	-	-	4
	Datos Esenciales						
7	Ficheros	3	4	3	-	-	3
8	Datos de Configuración	3	4	3	-	-	3
9	Datos de Validación de Credenciales	3	3	3	-	-	3
10	Datos de Control de Acceso	3	3	3	-	-	3
	Servicios Internos						
11	Acceso a Internet	3	-	-	-	-	3
12	Portal Electrónico	3	4	-	-	-	2
13	Acceso a Red Inalámbrica	3	1	3	-	-	2
	Equipamiento						
	Aplicaciones						
14	Ofimática	3	2	2	-	-	2
15	Sistema Operativo	4	3	3	-	-	3
16	Servidor de Servicios de Red	4	3	3	-	-	3
17	Servidor de Correos	4	3	3	-	-	3
18	Servidor Virtualizado SIGEA	4	3	3	-	-	3
19	Servidor Virtualizado Controlador de Dominio	4	3	3	-	-	3
20	Servidor Virtualizado SIAF	4	3	3	-	-	3
21	Servidor Virtualizado CPRESU	4	3	3	-	-	3
22	Servidor de Aplicaciones Web	4	3	3	-	-	3

	Equipos						
23	IBM SYSTEM-X3400M / Servidor de Correos	3	4	3	-	-	3
24	DELL POWEREDGE R720 / Servicios de Red	3	4	3	-	-	3
25	DELL POWEREDGE R420 / SIGEA y Controlador de Domir	3	4	3	-	-	3
26	DELL POWEREDGE R200 / Unidades Ejecutoras e intrane	3	4	3	-	-	3
27	HP SYSTEM 3200 / SIAF y CPRESU	3	4	3	-	-	3
28	Laptop	3	3	3	-	-	3
29	Computadores de Escritorio	3	3	3	-	-	3
30	Medios de Impresión	3	-	-	-	-	3
31	Switch	4	-	-	-	-	4
32	Access Point	4	-	-	-	-	4
33	Router	3	-	-	-	-	3
	Comunicaciones						
34	WIFI	3	3	3	-	-	3
35	Red de Área Local	3	3	3	-	-	3
36	Internet	3	3	3	-	-	3
	Elementos Auxiliares						
37	Equipos de Climatización	3	-	-	-	-	3
	Soporte de Información						
38	Disco Duro	4	2	4	-	-	3
39	**Instalaciones**						
40	Recinto	4	-	-	-	-	4
41	Instalaciones de respaldo	4	-	-	-	-	4

Anexo 6.7: Riesgo potencial

Valor	Criterio
5	Muy Alto
4	Alto
3	Medio
2	Bajo
1	Muy Bajo

Nº	Activos Activos Esenciales	[D]	[I]	[C]	[A]	[T]	% CR
	Servicios Esenciales						
1	SIGEA	3	3	3	-	3	3
2	SIAF	3	3	3	-	3	3
3	SIGA	3	3	3	-	3	3
4	CPRESU	3	3	3		3	3
5	Expedientes Administrativos Físicos	4	4	4	-	-	4
6	Acceso a Internet	4	-	-	-	-	4
	Datos Esenciales						
7	Ficheros	3	4	3	-	-	3
8	Datos de Configuración	3	3	4	-	-	3
9	Datos de Validación de Credenciales	3	3	3	-	-	3
10	Datos de Control de Acceso	3	3	3	-	-	3
	Servicios Internos						
11	Portal Electrónico	3	3	-	-	-	3
12	Acceso a Red Inalámbrica	4	2	2	-	-	3
	Aplicaciones						
13	Ofimática	4	3	-	-	-	4
14	Sistema Operativo	5	4	4	-	-	4
15	Servidor de Servicios de Red	4	4	4	-	-	4
16	Servidor de Correos	4	4	4	-	-	4
17	Servidor Virtualizado SIGEA	4	4	4	-	-	4
18	Servidor Virtualizado Controlador de Dom	4	4	4	-	-	4
19	Servidor Virtualizado SIAF	4	4	4	-	-	4
20	Servidor Virtualizado CPRESU	4	4	4	-	-	4
21	Servidor de Aplicaciones Web	4	4	4	-	-	4

	Equipos						
22	DELL POWEREDGE R720 / Servicios de Red	4	4	3	-	-	4
23	IBM SYSTEM-X3400M / Servidor de Correo	4	4	3	-	-	4
24	DELL POWEREDGE R420 / SIGEA y Controla	4	4	3	-	-	4
25	DELL POWEREDGE R200 / Unidades Ejecut	4	4	3	-	-	4
26	HP SYSTEM 3200 / SIAF y CPRESU	4	4	3	-	-	4
27	Laptop	4	3	3	-	-	3
28	Computadores de Escritorio	4	4	4	-	-	4
29	Medios de Impresión	4	-	-	-	-	4
30	Switch	3	-	-	-	-	3
31	Access Point	4	-	-	-	-	4
32	Router	3	-	-	-	-	3
	Comunicaciones						
33	WIFI	4	4	4	-	-	4
34	Red de Área Local	4	4	4	-	-	4
35	Internet	4	-	-	-	-	4
	Elementos Auxiliares						
36	Equipos de Climatización	3	-	-	-	-	3
	Soporte de Información						
37	Disco Duro	4	4	4	-	-	4
	Instalaciones						
38	Recinto	4	-	-	-	-	4
39	Instalaciones de respaldo	4	-	-	-	-	4

Anexo 6.8: Salvaguardas implementadas

Salvaguardas Implementadas		Situación
Backups	3 veces al día (1pm, tarde y noche)	Se almacena en el propio disco duro y en un equipo de respaldo que se ubica en la misma oficina a la vista de todos sobre el escritorio de un usuario.
Firewall Perimétrico Fortigate	Merma los ataques a través de políticas de usuario	Si detecta que un usuario está emitiendo más de 7mil o 15mil consultas bloquea la IP pública hasta q se disipe el ataque
Editor de Políticas	Al día a un usuario solo le permite enviar 200 correos por hora	Es importante evitar que el servidor caiga en lista negra, si eso sucede las instituciones que manejan listas negras pueden bloquearnos el servicio, no se podría enviar correos a Gmail, Hotmail, Yahoo u otros correos institucionales.
Motores Eléctricos	Garantizan la funcionalidad del servicio del internet	Otras instituciones dependen de los servicios de correo y sistemas.
Extintores	Garantizan seguridad ante incendios	Dependiendo de las oficinas por departamento se tienen uno o dos extintores.
Filtrado MAC	Mecanismo de seguridad para la red WIFI y control de acceso de navegación	Por defecto un usuario está restringido hasta que no se comunique lo contrario.
Plan de Contingencia	Con la finalidad de mantener la continuidad de los sistemas de información frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma.	
Plan de Mantenimiento Preventivo y Correctivo de Equipos de Computo	Mantener la continuidad operativa de los equipos informáticos.	

Anexo 6.9: Impacto residual

	Equipamiento										
	Aplicaciones										
11	Ofimática	E.1 Errores de los usuarios	N	3	4	3	2	0	-	-
12		E.12 Errores de mantenimiento o actualizaciones de programa	MF	5		3	3	3	-	-
13		A.4 Uso no previsto	F	4		1	1	1	-	-
14		E.11 Vulnerabilidades de los programas	MF	5		4	3	3	-	-
15	Sistema Operativo	I.3. Avería de origen físico o lógico	N	3	4	4	-	-	-	-
16		E.5 Difusión de software dañino	F	4		4	3	2	-	-
17		A.20 Ataques Informáticos	N	3		4	4	4	-	-
18		E.11 Vulnerabilidades de los programas	MF	5		5	4	4	-	-
19		A.19 Virus Informático	MF	5		4	3	3	-	-
20		E.12 Errores de mantenimieto o actualizaciones de programa	MF	5		5	4	-	-	-
21		A.4 Uso no previsto	F	4		4	3	3	-	-
22		E.1 Errores de los usuarios	F	4		4	3	3	-	-
23	Servidor de Servicios de Red	A.20 Ataques Informáticos	N	3	2	3	3	3	-	-
24	Servidor de Servicios de Red	A.13 Denegación de servicio (carga desmesurada de trabajo)	PF	2		2	-	-	-	-
25	Servidor de Correos	A.2 Suplantación de la identidad del usuario	N	3		-	3	3	3	-
26	Servidor Virtualizado SIGEA	E.11 Vulnerabilidades de los programas	MPF	1		2	2	2	-	-
27	Servidor Virtualizado Controlador de Don	A.19 Virus Informático	MPF	1		2	2	2	-	-
28	Servidor Virtualizado SIAF	E.2 Errores del administrador	N	3		3	3	3	-	-
29	Servidor Virtualizado CPRESU	E.12 Errores de mantenimiento o actualizaciones de programa	MPF	1		2	2	-	-	-
30	Servidor de Aplicaciones Web	A.6 Acceso no autorizado	N	3		-	4	4	-	-

N°	**Activos** / **Activos Esenciales** / Servicios Esenciales	Amenazas	Probabilidad Ocurrencia			[D]	[I]	[C]	[A]	[T]
			S	V	NPO					
1	Expedientes Administrativos Físicos	E.1 Errores de los usuarios	PF	2	3	3	4	3	-	-
2		A.11 Destrucción intencional de la información	N	3		4	-	-	-	-
3		I.1 Fuego	F	4		3	-	-	-	-
4		A.14 Robo	N	3		4	-	3	-	-
5		A.10 Modificación deliberada de la información	N	3		-	5	-	-	-
6	Acceso a Internet	I.6 Fallos de servicios de comunicaciones	F	4	3	4	-	-	-	-
7		A.13 Denegación de servicio (carga desmesurada de trabajo)	N	3		3	-	-	-	-
8		E.2 Errores del administrador	N	3		3	2	3	-	-
9		A.8 Repudio	PF	2		-	-	-	-	2
10		A.4 Uso no previsto	PF	2		2	0	0	-	-

	Equipamiento										
	Aplicaciones										
11	Ofimática	E.1 Errores de los usuarios	N	3	4	3	2	0	-	-
12		E.12 Errores de mantenimiento o actualizaciones de programa	MF	5		3	3	3	-	-
13		A.4 Uso no previsto	F	4		1	1	1	-	-
14		E.11 Vulnerabilidades de los programas	MF	5		4	3	3	-	-
15	Sistema Operativo	I.3. Avería de origen físico o lógico	N	3	4	4	-	-	-	-
16		E.5 Difusión de software dañino	F	4		4	3	2	-	-
17		A.20 Ataques Informáticos	N	3		4	4	4	-	-
18		E.11 Vulnerabilidades de los programas	MF	5		5	4	4	-	-
19		A.19 Virus Informático	MF	5		4	3	3	-	-
20		E.12 Errores de mantenimieto o actualizaciones de programa	MF	5		5	4	-	-	-
21		A.4 Uso no previsto	F	4		4	3	3	-	-
22		E.1 Errores de los usuarios	F	4		4	3	3	-	-
23	Servidor de Servicios de Red	A.20 Ataques Informáticos	N	3	2	3	3	3	-	-
24	Servidor de Servicios de Red	A.13 Denegación de servicio (carga desmesurada de trabajo)	PF	2		2	-	-	-	-
25	Servidor de Correos	A.2 Suplantación de la identidad del usuario	N	3		-	3	3	3	-
26	Servidor Virtualizado SIGEA	E.11 Vulnerabilidades de los programas	MPF	1		2	2	2	-	-
27	Servidor Virtualizado Controlador de Don	A.19 Virus Informático	MPF	1		2	2	2	-	-
28	Servidor Virtualizado SIAF	E.2 Errores del administrador	N	3		3	3	3	-	-
29	Servidor Virtualizado CPRESU	E.12 Errores de mantenimiento o actualizaciones de programa	MPF	1		2	2	-	-	-
30	Servidor de Aplicaciones Web	A.6 Acceso no autorizado	N	3		-	4	4	-	-

	Equipos										
31		I.2 Contaminación Mecánica (polvo, suciedad)	PF	2		2	-	-	-	-	
32		I.1 Fuego	PF	2		3	-	-	-	-	
33		I.3. Avería de origen físico o lógico	F	4		4	-	-	-	-	
34	IBM SYSTEM-X3400M / Servidor de Corre	I.4 Corte del suministro eléctrico	N	3		2	-	-	-	-	
35	DELL POWEREDGE R720 / Servicios de Re	I.5 Condiciones inadecuadas de temperatura o humedad	MF	5		4	-	-	-	-	
36	DELL POWEREDGE R420 / SIGEA y Contro	I.8 Degradación de los soportes de almacenamiento de informació	N	3		3	-	-	-	-	
37	DELL POWEREDGE R200 / Unidades Ejecu	E.13 Errores de mantenimiento o actualizacion de equipo (hardwa	F	4	3	4	-	-	-	-	
38	HP SYSTEM 3200 / SIAF y CPRESU	N.2 Desastres naturales	MPF	1		4	-	-	-	-	
39		E.2 Errores del administrador	N	3		3	3	3	-	-	
40		E.9 Destrucción de la información	PF	2		4	-	-	-	-	
41		A.18 Manipulación del hardware	MPF	1		4	-	2	-	-	
42		A.6 Acceso no autorizado	PF	2		-	4	2	-	-	
43		E.3 Errores de monitorización (actividad, log)	N	3		-	3	-	-	-	
44		E.1 Errores de los usuarios	F	4		2	2	2	-	-	
45		E.5 Difusión de software dañino	F	4		3	3	3	-	-	
46		I.2 Contaminación Mecánica (polvo, suciedad)	N	3		2	-	-	-	-	
47		E.9 Destrucción de la información	N	3		3	-	-	-	-	
48		I.5 Condiciones inadecuadas de temperatura	F	4		3	-	-	-	-	
49	Computadores de Escritorio	I.3. Avería de origen físico o lógico	N	3	4	4	-	-	-	-	
50		A.20 Ataques Informáticos	N	3		4	4	4	-	-	
51		I.1 Fuego	F	4		4	-	-	-	-	
52		A.6 Acceso no autorizado	N	3		-	4	4	-	-	
53		A.4 Uso no previsto	MF	5		3	3	3	-	-	
54		E.13 Errores de mantenimiento o actualizacion de equipo (hardwa	N	3		3	-	-	-	-	
55		I.7 Interrupción de otros servicios y suministros esenciales	MF	5		3	-	-	-	-	
56		E.13 Errores de mantenimiento o actualizacion de equipo (hardwa	PF	2		2	-	-	-	-	
57		A.6 Acceso no autorizado	MF	5		-	1	0	-	-	
58	Medios de Impresión	I.1 Fuego	N	3	4	4	-	-	-	-	
59		I.2 Contaminación Mecánica (polvo, suciedad)	N	3		2	-	-	-	-	
60		I.3. Avería de origen físico o lógico	F	4		4	-	-	-	-	
61		A.4 Uso no previsto	F	4		2	0	0	-	-	
62		E.1 Errores de los usuarios	F	4		3	1	0	-	-	
63		I.1 Fuego	PF	2		2	-	-	-	-	
64		I.2 Contaminación Mecánica (polvo, suciedad)	F	4		3	-	-	-	-	
65		I.3. Avería de origen físico o lógico	PF	2		3	-	-	-	-	
66	Access Point	A.14 Robo	MPF	1	3	5	-	-	-	-	
67		I.6 Fallos de servicios de comunicaciones	PF	2		3	-	-	-	-	
68		E.13 Errores de mantenimiento o actualizacion de equipo (hardwa	N	3		4	-	-	-	-	
	Comunicaciones										
69		E.2 Errores del administrador	N	3		2	3	3	-	-	
70		A.4 Uso no previsto	MPF	1		2	1	1	-	-	
71		A.6 Acceso no autorizado	N	3		-	3	3	-	-	
72	WIFI	I.6 Fallos de servicios de comunicaciones	N	3	3	4	-	-	-	-	
73		A.7 Análisis de tráfico	F	4		-	-	4	-	-	
74		A.9 Interceptación de información (escucha)	N	3		-	-	3	-	-	
75		A.2 Suplantación de la identidad del usuario	PF	2		-	3	3	3	-	
76		E.2 Errores del administrador	N	3		2	3	3	-	-	
77		A.6 Acceso no autorizado	MF	5		-	3	3	-	-	
78		I.6 Fallos de servicios de comunicaciones	N	3		4	-	-	-	-	
79	Red de Área Local	A.9 Interceptación de información (escucha)	N	3	3	-	-	3	-	-	
80		A.7 Análisis de tráfico	N	3		-	-	3	-	-	
81		A.4 Uso no previsto	PF	2		2	2	1	-	-	
82		E.2 Errores del administrador	PF	2		3	2	2	-	-	
83		I.6 Fallos de servicios de comunicaciones	N	3		3	-	-	-	-	
84	Internet	A.13 Denegación de servicio (carga desmesurada de trabajo)	N	3	3	3	-	-	-	-	
85		A.4 Uso no previsto	N	3		1	0	0	-	-	
	Soporte de Información										
86		I.1 Fuego	MPF	1		4	-	-	-	-	
87		E.14 Pérdida de equipos	F	4		5	-	5	-	-	
88		I.8 Degradación de los soportes de almacenamiento de informació	N	3		3	-	-	-	-	
89	Disco Duro	I.2 Contaminación Mecánica (polvo, suciedad)	N	3	4	3	-	-	-	-	
90		A.4 Uso no previsto	F	4		2	2	2	-	-	
91		A.14 Robo	F	4		5	-	5	-	-	
92		I.3. Avería de origen físico o lógico	MF	5		4	-	-	-	-	
	Instalaciones										
93		I.1 Fuego	N	3		3	-	-	-	-	
94	Recinto	N.1 Daños por agua	N	3		3	-	-	-	-	
95		N.3 Calor Extremo	F	4	3	4	-	-	-	-	
96	Instalaciones de respaldo	N.2 Desastres naturales	N	3		4	-	-	-	-	
97		A.15 Ataque destructivo (vandalismo, terrorismo)	N	3		3	-	-	-	-	

Anexo 6.10: Riesgo residual

Nº	Activos Activos Esenciales	[D]	[I]	[C]	[A]	[T]	% CR
	Servicios Esenciales						
1	Expedientes Administrativos Físicos	4	4	3	-	-	4
2	Acceso a Internet	3	-	-	-	-	3
	Datos Esenciales						
	Aplicaciones						
3	Ofimática	3	3	2	-	-	3
4	Sistema Operativo	4	4	3	-	-	4
5	Servidor de Servicios de Red	2	3	3	-	-	3
6	Servidor de Correos	2	3	3	-	-	3
7	Servidor Virtualizado SIGEA	2	3	3	-	-	3
8	Servidor Virtualizado Controlador de Dominio	2	3	3	-	-	3
9	Servidor Virtualizado SIAF	2	3	3	-	-	3
10	Servidor Virtualizado CPRESU	2	3	3	-	-	3
11	Servidor de Aplicaciones Web	2	3	3	-	-	3
	Equipos						
12	DELL POWEREDGE R720 / Servicios de Red	3	3	3	-	-	3
13	IBM SYSTEM-X3400M / Servidor de Correos	3	3	3	-	-	3
14	DELL POWEREDGE R420 / SIGEA y Controlador de Dominio	3	3	3	-	-	3
15	DELL POWEREDGE R200 / Unidades Ejecutoras e intranet	3	3	3	-	-	3
16	HP SYSTEM 3200 / SIAF y CPRESU	3	3	3	-	-	3
17	Computadores de Escritorio	3	3	3	-	-	3
18	Medios de Impresión	3	-	-	-	-	3
19	Access Point	3	-	-	-	-	3
	Comunicaciones						
20	WIFI	3	3	3	-	-	3
21	Red de Área Local	3	3	3	-	-	3
22	Internet	3	-	-	-	-	3
	Soporte de Información						
23	Disco Duro	4	4	4	-	-	4
	Instalaciones						
24	Recinto	3	-	-	-	-	3
25	Instalaciones de respaldo	3	-	-	-	-	3

Anexo 7: Vulnerabilidades lógicas

Vulnerabilidad	Información Vulnerabilidad	Puerto	Gravedad	Solución	Exploit SI / NO	Nombre
Adobe Flash Player	Detección de Adobe Flash Player Versión no compatible	445 tcp	Critica	Actualizar a una versión de Adobe Flash Player que es compatible actualmente	NO	
Plug and Play	MS05-039: Una vulnerabilidad en Plug and Play podría permitir la ejecución remota de código y elevación de privilegios (899588)	445 tcp	Critica	Parchar Windows	SI	Metasploit (MS05-039 Microsoft Plug and Play Servicio de desbordamiento)
Cola de impresión	MS05-043: Una vulnerabilidad en el servicio de cola de impresión podría permitir la ejecución remota de código (896423)	445 tcp	Critica	Parchar Windows	SI	Impacto Core
MSDTC y COM +	MS05-051: Vulnerabilidades en MSDTC y COM + podrían permitir la ejecución remota de código	445 tcp	Critica	Parchar Windows	SI	-
DNS	MS06-041: Una vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código	445 tcp	Critica	Parchar Windows	NO	-
TCP / IP	MS08-001: Vulnerabilidades en TCP / IP Windows podría permitir la ejecución remota de código	445 tcp	Critica	Parchar Windows	SI	LONA (CANVAS)/Impacto Core
Internet	MS09-071: Vulnerabilidades en Internet del Servicio de autenticación	445 tcp	Critica	Parchar Windows	NO	-
SMB	MS10-054: Vulnerabilidades en el servidor SMB	445 tcp	Critica	Parchar Windows	SI	Impacto Core
Oracle Java JDK / JRE 6	Oracle Java JDK / JRE 6	445 tcp	Critica	Actualizar para JDK / JRE 6 Update 20 o posterior y retire si es necesario las versiones afectadas	SI	Metasploit (Sun Java Web Start Plugin de línea de comandos de inyección Argumento
HyperTerminal	MS04-043: Vulnerabilidades en HyperTerminal (873339)	445 tcp	Alta	Parchar Windows	NO	-
kernel	MS05-018: Vulnerabilidades en kernel de Windows (890859)	445 tcp	Alta	Parchar Windows	SI	Impacto Core
Explorador de Windows	MS06-057: Una vulnerabilidad en el Explorador de Windows	445 tcp	Alta	Parchar Windows	SI	Metasploit (MS06-057 Microsoft Internet Explorer WebViewFolderIcon setSlice () Desbordamiento)
Microsoft Excel	MS08-014: Vulnerabilidades en Microsoft Excel	445 tcp	Alta	Parchar Windows	SI	Impacto Core
Schannel	MS14-066: Una vulnerabilidad en Schannel	3389 / tcp / msrdp	Alta	Parchar Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, y 2012 R2.	SI	Impacto Core
Remote Desktop	Microsoft Windows Remote Desktop Protocol Servidor	3389 /	Alta	Forzar el uso de SSL como una capa de	SI	-

Protocol	Man-in-the-Middle Debilidad	tcp / msrdp		transporte por este servicio si lo admite.		
SMB	Firma SMB Necesario	445 tcp	Alta	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft:	NO	-
Unquoted Enumeración Path	Servicio de Microsoft Windows Unquoted Enumeración Path	445 tcp	Alta	Asegúrese de que todos los servicios que contienen un espacio en la ruta encierran la ruta entre comillas.	SI	Metasploit (servicio de Windows Path Trusted Privilege Escalation)
Unquoted Enumeración Path	Servicio de Microsoft Windows Unquoted Enumeración Path	445 tcp	Alta	Asegúrese de que todos los servicios que contienen un espacio en la ruta encierran la ruta entre comillas.	SI	Metasploit (servicio de Windows Path Trusted Privilege Escalation)
Unquoted Enumeración Path	Servicio de Microsoft Windows Unquoted Enumeración Path	445 tcp	Alta	Asegúrese de que todos los servicios que contienen un espacio en la ruta encierran la ruta entre comillas.	SI	Metasploit (servicio de Windows Path Trusted Privilege Escalation)
SMB2	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback () Vulnerabilidad	445 tcp	Critica	Parchar Windows	SI	Metasploit (MS09-050 Microsoft SRV2.SYS SMB Negociar ProcessID Tabla Función Desreferencia)
SMB	MS10-012: Vulnerabilidades en SMB	445 tcp	Alta	Parchar Windows	SI	Impacto Core
SMB2	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback () Vulnerabilidad	445 tcp	Critica	Parchar Windows	SI	Metasploit (MS09-050 Microsoft SRV2.SYS SMB Negociar ProcessID Tabla Función Desreferencia)
Adobe Reader	Adobe Reader <10.1.10 / 11.0.07 Vulnerabilidades múltiples (APSB14-15)	445 tcp	Critica	Asciende a Adobe Reader 01.10.10 / 11.0.07 o posterior.	SI	-
Kaspersky	Kaspersky Anti-Virus Detección	445 tcp	Critica	Asegúrese de que las actualizaciones están funcionando y los servicios asociados se están ejecutando.	-	-
red de Windows	MS12-054: Vulnerabilidades en los componentes de red de Windows	445 tcp	Critica	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2.	-	Impacto Core
Oracle Java JDK / JRE 6	Oracle Java JDK / JRE 6	445 tcp	Critica	Actualizar para JDK / JRE 6 Update 20 o posterior y retire si es necesario las versiones afectadas	SI	Metasploit (Sun Java Web Start Plugin de línea de comandos de inyección Argumento
	Oracle Java SE Múltiples vulnerabilidades	445 tcp	Critica	Actualizar para JDK / JRE 5 Actualización 45, 6 Update 45, 7 Actualización 21 o posterior.	SI	Metasploit (Java Applet Tipo Reflexión Confusión ejecución remota de código)
Malware de microsoft	MS Seguridad Asesor 2974294: Una vulnerabilidad en el motor de protección contra Malware de microsoft	445 tcp	Alta	Activar las actualizaciones automáticas para actualizar el motor de exploración para las aplicaciones antimalware pertinentes.	-	-

.NET Framework	MS11-100: Vulnerabilidades en .NET Framework		Alta	Microsoft ha publicado un conjunto de parches para .NET Framework en Windows XP, 2003, Vista, 2008, 7 y 2008 R2.	SI	-
kernel	MS12-008: Vulnerabilidades en los controladores modo kernel de Windows	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2.	SI	-
Internet Explorer	MS14-021: Actualización de seguridad para Internet Explorer (2965111)	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para XP, 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, y 2012 R2.	SI	-
Windows Client	MS13-033: Una vulnerabilidad en Windows Client / servidor de tiempo de ejecución del subsistema	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista y 2008.	NO	-
shell de Windows	MS12-048: Una vulnerabilidad en el shell de Windows	445 tcp	Alta	Parchar Windows XP, 2003, Vista, 2008, 7 y 2008 R2.	NO	-
Escritorio remoto	MS12-020: Vulnerabilidades en Escritorio remoto	445 tcp	Alta	Parchar Windows XP, 2003, Vista, 2008, 7 y 2008 R2	SI	LONA (White_Phosphorus)
controles comunes de Windows	MS12-027: Una vulnerabilidad en controles comunes de Windows	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para Office 2003, 2007 y 2010, Office 2003 Web Components, SQL Server 2005 y 2008, BizTalk Server 2002, Visual FoxPro 8.0 y 9.0 y Visual Basic 6.0 Runtime	SI	ExploitHub (EH-14-562) - Metasploit (MS12-027 MSCOMCTL ActiveX Buffer Overflow)
Internet Explorer	MS12-037: Actualización de seguridad acumulativa para Internet Explorer (2699988)	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para XP, 2003, Vista, 2008, 7 y 2008 R2.	SI	Metasploit (MS12-037 Microsoft Internet Explorer Fijo desbordamiento Tabla Col Span Montón)
Adobe Flash Player	Múltiples vulnerabilidades	445 tcp	Alta	Actualiza a Flash Player versión 17.0.0.169 o posterior	SI	Metasploit (Adobe Flash Player Nellymoser Audio Decodificación de desbordamiento de búfer)
Kaspersky	Kaspersky Anti-Virus Detección	445 tcp	Critica	Asegúrese de que las actualizaciones están funcionando y los servicios asociados se están ejecutando.	-	-
Adobe Flash Player	Múltiples vulnerabilidades	445 tcp	Alta	SI	SI	SI
Unquoted Enumeración Path	Servicio de Microsoft Windows Unquoted Enumeración Path	445 tcp	Alta	Asegúrese de que todos los servicios que contienen un espacio en la ruta encierran la ruta entre comillas.	SI	Metasploit (servicio de Windows Path Trusted Privilege Escalation)
Microsoft Office	Microsoft Office Múltiples vulnerabilidades	445 tcp	Alta	SI	SI	SI
Kaspersky	Kaspersky Anti-Virus Detección	445 tcp	Critica	Asegúrese de que las actualizaciones están funcionando y los servicios asociados se están ejecutando.	-	-

Adobe Flash Player	Múltiples vulnerabilidades	445 tcp	Alta	Actualiza a Flash Player versión 17.0.0.169 o posterior	SI	Metasploit (Adobe Flash Player Nellymoser Audio Decodificación de desbordamiento de búfer)
Unquoted Enumeración Path	Servicio de Microsoft Windows Unquoted Enumeración Path	445 tcp	Alta	Asegúrese de que todos los servicios que contienen un espacio en la ruta encierran la ruta entre comillas	SI	Metasploit (servicio de Windows Path Trusted Privilege Escalation)
eliminación de Sofware mal intencionado de Microsoft	MS Seguridad Asesor 3074162: Una vulnerabilidad en Herramienta de eliminación de Sofware mal intencionado de Microsoft	445 tcp	Alta	Activar las actualizaciones automáticas para actualizar el motor de exploración para las aplicaciones antimalware pertinentes.	SI	-
Kaspersky	Kaspersky Anti-Virus Detección	445 tcp	Critica	Asegúrese de que las actualizaciones están funcionando y los servicios asociados se están ejecutando.	-	-
red de Windows	MS12-054: Vulnerabilidades en los componentes de red de Windows	445 tcp	Critica	Parchar Windows XP, 2003, Vista, 2008, 7 y 2008 R2.	-	Impacto Core
Remote Procedure Call	MS13-062: Una vulnerabilidad en Remote Procedure Call	445 tcp	Critica	Parchar Windows XP, 2003, Vista, 2008, 7, 2008 R2, 8, y 2012	-	-
Adobe Flash Player	Múltiples vulnerabilidades	445 tcp	Alta	Actualiza a Flash Player versión 17.0.0.169 o posterior	SI	Metasploit (Adobe Flash Player Nellymoser Audio Decodificación de desbordamiento de búfer)
Google Chrome	Google Chrome 45.0.2454.85 <Múltiples vulnerabilidades	445 tcp	Alta	Actualizar a Google Chrome 45.0.2454.85 o posterior	NO	-
Unquoted Enumeración Path	Servicio de Microsoft Windows Unquoted Enumeración Path	445 tcp	Alta	Asegúrese de que todos los servicios que contienen un espacio en la ruta encierran la ruta entre comillas	SI	Metasploit (servicio de Windows Path Trusted Privilege Escalation)
kernel	MS12-008: Vulnerabilidades en los controladores modo kernel de Windows	445 tcp	Alta	Parchar Windows XP, 2003, Vista, 2008, 7 y 2008 R2.	SI	-
Escritorio remoto	MS12-020: Vulnerabilidades en Escritorio remoto	445 tcp	Alta	Parchar Windows XP, 2003, Vista, 2008, 7 y 2008 R2	SI	LONA (White_Phosphorus)
vulnerabilidad en Windows	MS12-024: Una vulnerabilidad en Windows	445 tcp	Alta	Parchar Windows XP, 2003, Vista, 2008, 7 y 2008 R2	SI	-
controles comunes de Windows	MS12-027: Una vulnerabilidad en controles comunes de Windows	445 tcp	Alta	Instalar parches para Office 2003, 2007 y 2010, Office 2003 Web Components, SQL Server 2005 y 2008, BizTalk Server 2002, Visual FoxPro 8.0 y 9.0 y Visual Basic 6.0 Runtime	SI	ExploitHub (EH-14-562) - Metasploit (MS12-027 MSCOMCTL ActiveX Buffer Overflow)
Windows Client	MS13-033: Una vulnerabilidad en Windows Client / servidor de tiempo de ejecución del subsistema	445 tcp	Alta	Instalar parches Windows XP, 2003, Vista y 2008.	NO	-
kernel	MS13-063: Vulnerabilidades en kernel de Windows	445 tcp	Alta	Instalar parches Windows XP, 2003, Vista y	NO	-

				2008.		
Internet Explorer	MS13-069: Actualización de seguridad acumulativa para Internet Explorer (2870699)	445 tcp	Alta	Instalar Windows XP, 2003, Vista y 2008.	SI	Metasploit (MS13-069 Microsoft Internet Explorer CCaret Uso-Abierto gratuito)
archivo de tema	MS13-071: Una vulnerabilidad en Windows archivo de tema	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista y 2008.	SI	Metasploit (MS13-071 de Microsoft Windows File temático Manejo ejecución de código arbitrario)
Internet Explorer	MS13-080: Actualización de seguridad acumulativa para Internet Explorer (2879017)	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para XP, 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, y 2012 R2	SI	Metasploit (MS13-080 Microsoft Internet Explorer CDisplayPointer Uso-Abierto gratuito)
kernel	MS13-081: Vulnerabilidades en los controladores modo kernel de Windows	445 tcp	Alta	Instalar parches Windows XP, 2003, Vista, 2008, 7, 2008 R2, 8, Windows RT, y 2012.	SI	Metasploit (Windows TrackPopupMenuEx Win32k NULL página)
Internet Explorer	MS14-021: Actualización de seguridad para Internet Explorer (2965111)	445 tcp	Alta	Actualizar software.	SI	-
manejo de archivos de Windows	MS14-019: Una vulnerabilidad en el componente de manejo de archivos de Windows	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, y 2012 R2.	NO	-
Escritorio remoto	MS12-020: Vulnerabilidades en Escritorio remoto	445 tcp	Alta	Parchar Windows.	SI	LONA (White_Phosphorus)
SMB	MS09-001: Microsoft Windows SMB vulnerabilidades de ejecución remota de código	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.	SI	Metasploit (Microsoft SRV.SYS WriteAndX válida DataOffset)
Unquoted Enumeración Path	Servicio de Microsoft Windows Unquoted Enumeración Path	445 tcp	Alta	Asegúrese de que todos los servicios que contienen un espacio en la ruta encierran la ruta entre comillas	SI	Metasploit (servicio de Windows Path Trusted Privilege Escalation)
Kaspersky	Kaspersky Anti-Virus Detección	445 tcp	Critica	Asegúrese de que las actualizaciones están funcionando y los servicios asociados se están ejecutando.	-	-
Remote Procedure Call	MS13-062: Una vulnerabilidad en Remote Procedure Call	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7, 2008 R2, 8, y 2012.	NO	-
FLEXnet Connect Service	Código múltiple FLEXnet Connect Service Actualizar ActiveX Control de vulnerabilidades en ejecución	445 tcp	Alta	Actualiza a la versión 6.0.100.65101 o posterior del cliente FLEXnet Connect	SI	Metasploit (Macrovision InstallShield Update Service ActiveX inseguros Método)
servicio de Windows	Permisos inseguros de servicio de Windows	445 tcp	Alta	Además, asegúrese de que estos grupos no tienen permiso de control total a los directorios que contienen los ejecutables de	-	-

				servicio.		
Unquoted Enumeración Path	Servicio de Microsoft Windows Unquoted Enumeración Path	445 tcp	Alta	Asegúrese de que todos los servicios que contienen un espacio en la ruta encierran la ruta entre comillas	SI	Metasploit (servicio de Windows Path Trusted Privilege Escalation)
protección contra el malware de microsoft	MS Seguridad Asesor 2974294: Una vulnerabilidad en el motor de protección contra el malware de microsoft	445 tcp	Alta	Activar las actualizaciones automáticas para actualizar el motor de exploración para las aplicaciones antimalware pertinentes.	NO	-
Herramienta de eliminación de Sofware mal intencionado de Microsoft	MS Seguridad Asesor 3074162: Una vulnerabilidad en Herramienta de eliminación de Sofware mal intencionado de Microsoft	445 tcp	Alta	Activar las actualizaciones automáticas para actualizar el motor de exploración para las aplicaciones antimalware pertinentes.	SI	-
Microsoft Excel	MS07-023,036 MS08-014,043,074 MS09-021,067 MS10-017,038 MS10-057,080 MS11-021	445 tcp	Alta	SI	SI	SI
Microsoft Publisher	MS08-012,027	445 tcp	Alta	SI	SI	SI
Microsoft Word	MS08-026,072 MS09-027,068 MS10-056,079	445 tcp	Alta	SI	SI	SI
.NET Framework	MS11-028,044,078 MS12-016,025,035,038,074	445 tcp	Alta	SI	SI	SI
kernel	MS12-075: Una vulnerabilidad en el kernel de Windows-Mode Drivers	445 tcp	Alta	Instalar parches para Windows XP, 2003, Vista, 2008, 7, 2008 R2, 8, y 2012.	SI	Impacto Core
Internet Explorer	MS13-008: Actualización de seguridad para Internet Explorer (2799329)	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para XP, 2003, Vista, 2008, 7, 2008 R2.	SI	Metasploit (vulnerabilidad MS13-008 Microsoft Internet Explorer CButton Objeto Uso-Abierto gratuito)
kernel	MS13-081: Vulnerabilidades en los controladores modo kernel de Windows	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7, 2008 R2, 8, Windows RT.	SI	Metasploit (Windows TrackPopupMenuEx Win32k NULL página)
archivo de tema	MS13-071: Una vulnerabilidad en Windows archivo de tema	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista y 2008	SI	Metasploit (MS13-071 de Microsoft Windows File temático Manejo ejecución de código arbitrario)
Unquoted Enumeración Path	Servicio de Microsoft Windows Unquoted Enumeración Path	445 tcp	Alta	Asegúrese de que todos los servicios que contienen un espacio en la ruta encierran la ruta entre comillas	SI	Metasploit (servicio de Windows Path Trusted Privilege Escalation)
SMB	MS10-012: Vulnerabilidades en SMB	445 tcp	Critica	Instalar parches para Windows 2000, XP, 2003, Vista, 2008, 7 y 2008 R2.	SI	Impacto Core
servicio de Windows	Permisos inseguros de servicio de Windows	445 tcp	Alta	Asegúrese de que los grupos no tienen permiso de control total a los directorios que	-	-

				contienen los ejecutables de servicio.		
Unquoted Enumeración Path	Servicio de Microsoft Windows Unquoted Enumeración Path	445 tcp	Alta	Asegúrese de que todos los servicios que contienen un espacio en la ruta encierran la ruta entre comillas	SI	Metasploit (servicio de Windows Path Trusted Privilege Escalation)
SMB	MS11-048: Una vulnerabilidad en el servidor SMB podría permitir la denegación de servicio	445 tcp	Alta	Microsoft ha publicado un conjunto de parches para Vista, 2008, 7 y 2008 R2	SI	Impacto Core

Anexo 8: Vulnerabilidades físicas

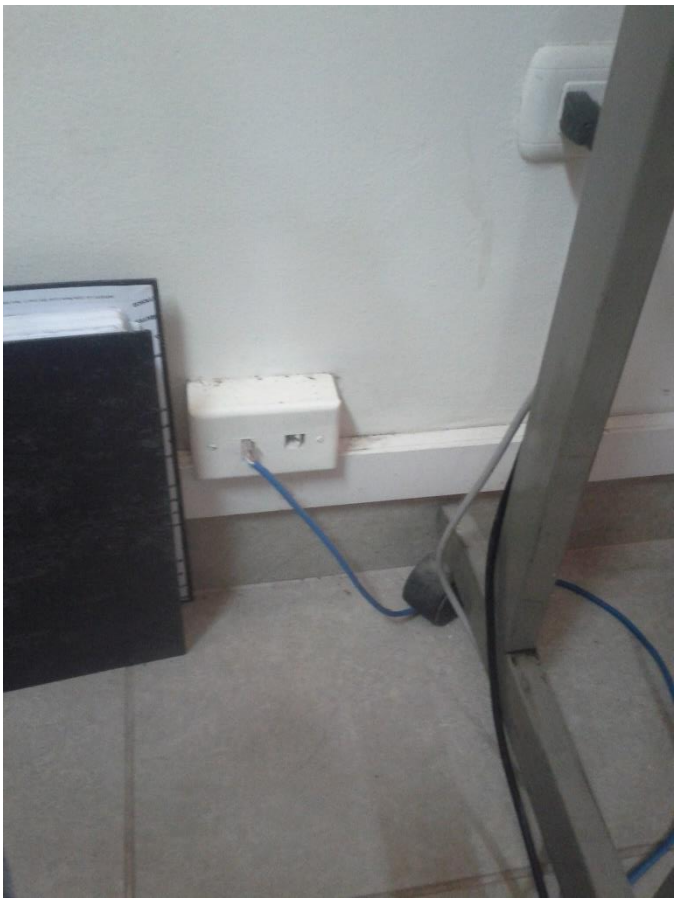
Riesgo de Fuego e incendio al rack de pared y sus componentes.
Fuente: GRP

Riesgo de Fuego e incendio de los documentos o expedientes físicos.
Fuente: GRP

Riesgo de Fuego e incendio de recursos físicos.
Fuente: GRP

Riesgo de Fuego e incendio total o parcial de los recursos de información.
Fuente: GRP

Riesgo de Fuego e incendio total o parcial de los recursos de información y elementos auxiliares.
Fuente: GRP



Puntos de red LAN desprotegidos.
Fuente: GRP

Anexo 9: Propuesta de salvaguardas

Activos Esenciales / Servicios Esenciales	Amenazas	Salvaguardas	Tipo de Salvaguarda
Expedientes Administrativos Físicos	E.1 Errores de los usuarios	Charla de concienciación a los usuarios sobre el uso y ubicación de los expedientes físicos y puntos eléctricos. Capacitación sobre Salud y Seguridad en el trabajo.	Prevención
	A.11 Destrucción intencional de la información		
	I.1 Fuego		
	A.14 Robo		
	A.10 Modificación deliberada de la información		
Acceso a Internet	I.6 Fallos de servicios de comunicaciones	Aseguramiento de la disponibilidad del acceso a internet - Análizar si la banda ancha actual satisface la demanda de peticiones web. - Mantenimiento preventivo a los Access Point, Router, Switch.. - Adquirir dispositivos Access Point y Router como reserva.	Prevención
	A.13 Denegación de servicio (carga desmesurada de trabajo)	Protección de las comunicaciones.	Prevención
Aplicaciones			
Ofimática	A.4 Uso no previsto	Herramienta contra código dañino.	Administración
	E.12 Errores de mantenimiento o actualizaciones de programa	Configuración de actualizaciones automáticas de Windows Update.	Administración
	E.11 Vulnerabilidades de los programas	Actualización de ficheros.	Administración
Sistema Operativo	I.3. Avería de origen físico o lógico	Actualización de ficheros.	Administración
	E.5 Difusión de software dañino	Protección de las aplicaciones informáticas - Actualización del Antivirus Kaspersky en todos los ordenadores. - Concienciación al usuario sobre las consecuencias del software o aplicaciones no autorizadas.	Prevención
	E.11 Vulnerabilidades de los programas	Aseguramiento de la integridad de datos - Configuración de Windows Update. - Instalación de parches publicados por Microsoft.	Prevención
	E.12 Errores de mantenimieto o actualizaciones de programa	Aseguramiento de la disponibilidad de datos - Configuración de actualizaciones automáticas de Windows Update.	Prevención
	A.4 Uso no previsto	Programación y ejecución de Copias de seguridad en la nube.	Recuperación

Servidor de Servicios de Red Servidor de Correos Servidor Virtualizado SIGEA	A.20 Ataques Informáticos E.11 Vulnerabilidades de los programas E.12 Errores de mantenimiento o actualizaciones de programa	Configuracón de Windows Update - Instalación de parches publicados por Microsoft.	Administración, Prevención
Servidor Virtualizado Controlador de Servidor Virtualizado SIAF Servidor Virtualizado CPRESU	A.13 Denegación de servicio (carga desmesurada de trabajo) A.6 Acceso no autorizado	Aseguramiento de la disponibilidad. Análisis de vulnerabilidades.	Prevención Administración
Servidor de Aplicaciones Web		HoneyPot -Honeynet.	Disuasoria
Equipos			
DELL POWEREDGE R720 / Servicios IBM SYSTEM-X3400M / Servidor de	I.5 Condiciones inadecuadas de temperatura o humedad I.4 Corte del suministro eléctrico I.8 Degradación de los soportes de almacenamiento de información	Aseguramiento de la disponibilidad - Equipos de enfriamiento. - Ventiladores directos a la fuente generadora de calor de los servidores. - Ubicación estandarizada de los equipos que garantizen la disipación adecuada de calor. - Asimilación de la ISO 942. Es necesario dar mantenimiento a los UPS y asegurar su disponibilidad.	Prevención Prevención
DELL POWEREDGE R420 / SIGEA y Controlador de Dominio	E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	Mantenimiento de equipos - Analizar la vida util de los equipos por la inadecuada temperatura y el mantenimiento o cambio del mismo.	Prevención
DELL POWEREDGE R200 / Unidades	E.2 Errores del administrador	Segregación de tareas	Prevención
HP SYSTEM 3200 / SIAF y CPRESU	E.9 Destrucción de la información A.18 Manipulación del hardware A.6 Acceso no autorizado	- Copias de Seguridad alojadas en sitios externos. - Camaras de seguridad. - Reloj Biométrico (control de acceso). - Asimilación de la ISO 942.	Prevención, Recuperación
	A.13 Denegación de servicio (carga desmesurada de trabajo)	Herramienta contra código dañino.	Prevención
	E.3 Errores de monitorización (actividad, log)	Análisis de los registros de actividad.	Monitorización

Computadores de Escritorio	E.1 Errores de los usuarios	- Charla de concienciación al usuario sobre las consecuencias del software dañino. - Charla de concienciación al usuario sobre la importancia del uso del	Concienciación, Prevención
	E.5 Difusión de software dañino		
	I.5 Condiciones inadecuadas de temperatura	Aseguramiento de la disponibilidad - Equipos de enfriamiento.	Prevención
	A.20 Ataques Informáticos	Configuracón de Windows Update - Instalación de parches publicados por Microsoft.	Administración, Prevención
	I.1 Fuego	- Charla de concienciación a los usuarios sobre el uso y ubicación de los puntos eléctricos.	Prevención
	A.6 Acceso no autorizado	- Charla de concienciación al usuario sobre las consecuencias del acceso no autorizado a su computadora.	Concienciación
	A.4 Uso no previsto	Concienciación al usuario sobre la ralentización del ordenador por procesos extras o tareas que no corresponden al ejercicio laboral.	Concienciación
	E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	- Ejecutar el mantenimiento preventivo y correctivo de los equipos de computo.	Prevención
Medios de Impresión	I.7 Interrupción de otros servicios y suministros esenciales	Aseguramiento de la disponibilidad - Ejecutar el mantenimiento preventivo y correctivo de equipos de computo.	Prevención
	I.2 Contaminación Mecánica (polvo, suciedad)		
	I.1 Fuego	Aseguramiento de la disponibilidad - Coordinar la importancia de una correcta ubicación de archivos fisicos y puntos eléctricos. - Capacitación en Salud y Seguridad en el trabajo.	Prevención
	E.13 Errores de mantenimiento o actualizacion de equipo (hardware)	Mantenimiento de equipos.	Prevención
	I.3. Avería de origen físico o lógico	- Directiva de renovación de equipos. - Evaluar la opción de alquilar los equipos, el proveedor dará soporte por averías físicas y mantenimiento preventivo.	Prevención
Access Point	I.1 Fuego	Aseguramiento de la disponibilidad - Coordinar la importancia de una correcta ubicación de archivos fisicos y puntos eléctricos.	Prevención
	I.2 Contaminación Mecánica (polvo, suciedad)	Aseguramiento de la disponibilidad - Ejecutar el mantenimiento preventivo y correctivo de equipos de computo.	Prevención
	E.13 Errores de mantenimiento o actualizacion de equipo (hardware)		
	I.6 Fallos de servicios de comunicaciones		

Comunicaciones			
WIFI	E.2 Errores del administrador	Coordinación en bajas de acceso a usuarios externos.	Eliminación
	A.6 Acceso no autorizado	Auditar la red WI-FI.	Prevención
	I.6 Fallos de servicios de comunicaciones	Aseguramiento de la disponibilidad del servicio - Mantenimiento preventivo a los Access Point.	Prevención
	A.7 Análisis de tráfico	Medios de encriptación de datos.	Administración
	A.9 Interceptación de información (escucha)		
	A.2 Suplantación de la identidad del usuario	Escaneo de host vivos en la red inalámbrica.	Administración
Red de Área Local	E.2 Errores del administrador	Directivas de uso de puntos de red.	Concienciación
	A.6 Acceso no autorizado	Restricción de laptops personales.	Limitación del Impacto
		Gabinetes de piso para los switch en las oficinas.	Administración
	I.6 Fallos de servicios de comunicaciones	Aseguramiento de la disponibilidad.	Prevención
	A.9 Interceptación de información (escucha)	Medios de encriptación de datos.	Prevención
	A.7 Análisis de tráfico		
Soporte de Información			
Disco Duro	I.1 Fuego	Inspecciones de seguridad.	Prevención
	E.14 Pérdida de equipos	Protección de los soportes de información.	Prevención
	I.8 Degradación de los soportes de almacenamiento de información	Protección del Hardware.	Prevención
	A.14 Robo	Programación y ejecución de Copias de seguridad en la nube.	Prevención
	I.3. Avería de origen físico o lógico	Aseguramiento de la disponibilidad.	Prevención
Instalaciones			
Recinto Instalaciones de respaldo	N.3 Calor Extremo N.2 Desastres naturales	Climatización.	Limitación del Impacto
		Planificación de seguridad.	Correccion
		Inspecciones de seguridad.	Prevención

Anexo 10: Guías de observación

GUÍA DE OBSERVACIÓN Nº 01
Identificación Y Valoración de Activos de Información

Código	Descripción del Activo de Información	Tipo	Propietario	Servicio	Características	Versión/ OS	N°

Código	Activos de Información	Dimensiones				
		D	I	C	A	T

GUÍA DE OBSERVACIÓN Nº 02
Identificación y valoración de amenazas asociadas a los activos de información

Código de Activos Inf.	Amenazas	Probabilidad Ocurrencia		Dimensiones				
		S	V	D	I	C	A	T

GUÍA DE OBSERVACIÓN Nº 03
Identificación de salvaguardas

Salvaguarda	Descripción	Situación

GUÍA DE OBSERVACIÓN Nº 04

Escaneo de vulnerabilidades de las computadoras instaladas en el Gobierno Regional Piura.

Objetivo: Identificar las vulnerabilidades que se encuentran en las computadoras.

Host: _____

IP: _____

MAC: _____

Nombre de Dominio o Grupo: _____

Sistema Operativo: _____

Fecha y Hora: _____

ID	Vulnerabilidad	Puerto	Tipo	Criticidad	Exploit

Anexo 11: Plan de mantenimiento preventivo de equipos informáticos

PLAN DE MANTENIMIENTO PREVENTIVO DE EQUIPOS INFORMÁTICOS EN EL GOBIERNO REGIONAL PIURA

I. PRESENTACIÓN

El área de Soporte Técnico de la Oficina de Tecnologías de la Información del Gobierno Regional Piura, tiene como función realizar el mantenimiento preventivo de los equipos informáticos, asimismo realizar una limpieza de software que permita depurar los programas no autorizados.

El objetivo principal de establecer un plan de mantenimiento preventivo es garantizar que los recursos informáticos cumplan con las funciones requeridas durante su ciclo de vida útil, mejorando aspectos operativos relevantes del establecimiento tales como funcionalidad, seguridad, productividad, confort, imagen y racionalizar costos de operación.

El mantenimiento debe ser periódico y permanente permitiendo evitar o mitigar las consecuencias de los fallos de equipos, previniendo las incidencias antes de que estas ocurran.

II. DIAGNÓSTICO SITUACIONAL

El Gobierno Regional Piura cuenta con 2 locales a los cuales conoceremos como local de Presidencia y local de Infraestructura.
Según el inventario realizado a inicios del presente año, la organización cuenta con los siguientes equipos:

2.1 Local de presidencia

- Hardware

  a) 173 Computadoras

  b) 43 Laptop

  c) 36 Impresoras chicas y 22 impresoras grandes

d) 10 Escáner

e) 05 Fotocopiadoras

- Comunicaciones

  a) 18 Switch

  b) 01 HUB

  c) 06 Access Point

2.2 Local de infraestructura

- Hardware

  a) 367 Computadoras

  b) 35 laptops

  b) 86 Impresoras

  c) 08 UPS

- Comunicaciones

  a) 29 Switch

  b) 01 HUB

  c) 03 Access Point

III. JUSTIFICACIÓN

Es necesario realizar y programar un mantenimiento preventivo de los equipos informáticos permitiendo un correcto funcionamiento del hardware y software. La ausencia del mismo puede generar comportamientos inestables haciéndolos propensos a sufrir daños a largo plazo, requiriendo su reparación y la reducción de su vida útil.

El polvo almacenado en las partes del hardware genera un flujo de la electricidad estática, ocasionando la no operatividad del equipo, además puede formar una capa térmica que eleva la temperatura y reduce el tiempo de vida del equipo o en el peor de los casos puede quemar los componentes internos.

La suciedad de los periféricos (teclado, mouse y los botones del monitor), es

propicia para la proliferación de gérmenes, bacterias y virus causantes de infecciones, pudiendo tener un efecto negativo en la productividad laboral.

IV. OBJETIVO GENERAL

Realizar un mantenimiento preventivo para mantener la continuidad operativa de los equipos informáticos.

Objetivos específicos

- Realizar un cronograma de las actividades para la ejecución del mantenimiento preventivo.
- Disminuir costos por averías de los equipos informáticos.
- Actualizar el inventario de equipos informáticos.

V. AMBITO DE APLICACIÓN

Se aplicará a los dos locales, donde se encuentren instalados los equipos informáticos pertenecientes al Gobierno Regional Piura.

VI. PROCEDIMIENTO

a) Equipos de cómputo

Se realizará teniendo en cuenta dos aspectos:

- Los equipos informáticos que están fuera de la garantía, será realizado por personal del área de Soporte Técnico, es decir pruebas, ajustes, reemplazo, calibración y reinstalación.
- Los equipos informáticos que se encuentran dentro de la garantía, el mantenimiento se solicitará a la empresa en donde se adquirió el bien, y se hará el seguimiento de acuerdo a los contratos estipulados de las adquisiciones.

Para realizar el mantenimiento respectivo de los equipos informáticos se debe considerar cada uno de los siguientes componentes:

- CPU
- Monitor

- Teclado
- Mouse
- Impresora
- Equipos De Comunicación
- Red

1) CPU: Limpiar la fuente de alimentación, placa madre, disco duro, lectora de CD, memoria RAM y lubricar los cooler internos.
2) Monitor: Se hará una limpieza externa del mismo, quitando todo exceso de polvo
3) Teclado: Se limpia todo resto extraño que se encuentre al interior de las teclas. De estar presentando problemas se debe informar con ficha técnica para su reposición.
4) Mouse: Abrir y limpiar el mecanismo, de estar presentando problemas se debe informar con ficha técnica para su reposición.
5) Switch: Eliminación de polvo con la compresora de aire.
6) Red: Verificación del estado de los conectores y testeo de señal de red.

Al terminar el mantenimiento preventivo el personal responsable del servicio tendrá que comprobar el correcto funcionamiento de los equipos.

b) Impresoras

El mantenimiento preventivo consiste solo en limpieza externa, en caso de requerir un mantenimiento correctivo es recomendable que sea realizado por personal especializado en la marca, esto significa un servicio externo a la institución.

c) Fotocopiadoras

El mantenimiento preventivo consiste solo en limpieza externa, en caso de requerir un mantenimiento correctivo es recomendable que sea realizado por personal especializado en la marca, esto significa un servicio externo a la institución.

d) Escáner

Se hará una limpieza externa del mismo, quitando todo exceso de polvo.

VII. MATERIAL Y PRESUPUESTO

Para la ejecución se requiere del siguiente material:

- 01 ciento de Guantes
- 01 ciento de mascarillas protectoras
- 04 spray limpia contactos.
- 03 brochas de 2" de cerdas largas.
- 02 galones de alcohol Isopropílico.
- 02 frasco de lubricante para impresoras.
- 02 grasa para engranaje del sistema mecánico de impresoras.
- 06 pulseras antiestáticas.
- 01 millar de papel DIN A4
- 20 kilos de Trapo industrial

VIII. RECOMENDACIONES

1. Gestionar el requerimiento total del material requerido.
2. Gestionar con las jefaturas correspondientes a fin de comunicar al usuario sobre el cronograma de ejecución del mantenimiento preventivo de los equipos de cómputo.
3. Comunicar a las jefaturas sobre posibles imprevistos que pudieran ocurrir en el proceso del mantenimiento preventivo de los equipos informáticos.

Anexo 12: Propuesta de implementación de data center

PROPUESTA DE IMPLEMENTACIÓN DE DATA CENTER EN EL GOBIERO REGIONAL PIURA

I. ANTECEDENTES

El Gobierno Regional Piura actualmente cuenta con una sala de comunicaciones que no brinda garantías de disponibilidad, integridad y confidencialidad de datos. Es por ello que se presenta la siguiente propuesta para la implementación de un nuevo Data Center alineado a la ISO 942.

II. REQUERIMIENTO

a) Infraestructura
b) Electricidad
c) Refrigeración
d) Seguridad y monitoreo ambiental
e) Puesta en marcha

III. PLANTEAMIENTO TÉCNICO

1. Descripción general

Se propone evaluar un nuevo ambiente para la implementación del nuevo Data Center, según la ISO 942 como requerimiento mínimo requiere un área de 30 m2.

Detallando la parte operativa es necesario instalar en la parte eléctrica una Nueva Acometida, tendida desde el grupo del tablero general. Instalar un tablero eléctrico nuevo que permita el control de los equipos de aire acondicionado e iluminación.

Instalar un sistema de puesta a tierra independiente, de cero mantenimientos y resistividad > a 5 OHM.

Instalar un sistema de aire acondicionado de precisión, que permita controlar la refrigeración de los gabinetes de los servidores y comunicaciones.

Se recomienda la instalación de una caja de seguridad que permita la protección de documentos confidenciales y/o equipos que requieran estricta protección.

Se debe considerar el sistema de control de monitoreo con cámaras, control ambiental y seguridad, así como el control biométrico de acceso al área y el suministro de los extintores para ambientes electrónicos.

2. Detalle técnico

2.1 Infraestructura

a) Picado de piso.
b) Acabado en pintura con retarde anti fuego.
c) Cielo raso en baldosa de 60x60.

2.2 Electricidad

a) Acometidas

Se empelará como conductor de energía de cable cero alógenos tipo NH-80 para conductores que transportan corriente y el conductor de enlace a tierra será de tipo CPT.

En el recorrido del cableado eléctrico estará cubierto por tubería EMT de 2".

b) Tablero de Distribución Comercial

Se propone implementar un tablero donde se controlarán los equipos de aire acondicionado y las luminarias.

c) Tablero de Distribución Estabilizada (DATA CENTER)

Se propone implementar un solo tablero estabilizado donde controlará las salidas de los UPS, el tablero estará dividido en dos partes, la parte superior será controlada por el UPS N°1 y la parte inferior por el UPS N°2.

Será del tipo adosable con gabinete metálico con grado de protección IP44, placa base, mandil abisagrado y puerta con chapa plush. En su interior alojará dos paneles de distribución de 12 polos monofásicos con barras de cobre pintadas acorde con los colores descrito en el Código Nacional de Electricidad.

d) Sistema de Puesta a Tierra

El sistema de puesta a tierra debe ser en cemento conductivo libre de mantenimiento con resistividad > 5 OHM.

e) Iluminación

Se recomienda 4 equipos LED + 2 equipos de luces de emergencia.

2.3 Refrigeración

a) Aire Acondicionado de Precisión

Solución APC de aire acondicionado InRow.

- InRow SC, 300mm, Air Cooled, Self-contained 200-240V 60Hz.
- Sensor de aniego.
- Incluye Start UP brindado por la marca.
- Incluye mantenimiento anual.
- Incluye instalación inicial.

b) Aire Acondicionado de Backup

Se recomienda adquirir un equipo de aire acondicionado como backup.

2.4 Seguridad, Control de Acceso, Monitoreo y Control Ambiental

a) Seguridad

- Puerta corta-fuego metálica con acabado electroestática.
- Caja de seguridad montada y reforzada con pintura anti-flama.
- Extintor para incendios Clase C.

b) Control de Acceso

- Sistema de control de acceso biométrico, clave y tarjeta de proximidad.
- Monitoreo por conexión TCP/IP.
- Cerradura electromagnética.
- Pulsador de apertura interno.

c) Monitoreo y Vigilancia

- NVR con capacidad de 4 cámaras y discos duros de 30 días de almacenamiento.
- 3 cámaras IP de 720px.
- Servicio de instalación y configuración.
- Permite monitoreo remoto.

d) Control Ambiental

- Configuración de alerta por correo ante eventos de temperatura, humedad y aniego.
- Sensor de humo con sirena externa que permita una alerta Sonora ante un incendio.

IV. PROPUESTA ECONÓMICA

COSTO IMPLEMENTACIÓN DE DATA CENTER GOBIERNO REGIONAL PIURA
REFERENCIA: CONSTRUCCIÓN Y ACONDICIONAMIENTO DE DATACENTER
PROVEEDOR: COSUR SOLUCIONES INTEGRALES SAC

ITEM	DESCRIPCION	UNID	CANTIDAD	COSTO UNITARIO S./	COSTO TOTAL S./
1.0	**OBRAS CIVILES PREVIAS:**				
1.2	SEÑALIZACION DE ZONA DE TRABAJO Y SISTEMA DE SEGURIDAD (MALLAS Y CINTAS DE SEGURIDAD)	GLB	1	S/. 350.00	S/. 350.00
2.0	**CONSTRUCCION DE PAREDES CONCRETO 30M2**				
2.1	SUMINISTRRO DE MATERIALES (LADRILLOS, MORTERO, ARENA FINA, ARENA GRUESA, CEMENTO)	GLB	1	S/. 1,450.00	S/. 1,450.00
2.2	PINTADO GENERAL DEL AMBIENTE INTERNO Y EXTERNO (INC. PINTURA RETARDANTE IGNIFUGA Y EMPASTE)	M2	67.2	S/. 26.00	S/. 1,747.20
2.3	MANO DE OBRA DE ALBAÑILERIA (CONSTRUCCION, INS. LADRILLO, TARRAJEO Y ACABADO)	M2	28.84	S/. 20.00	S/. 576.80
3.0	**SUMINISTRO E INSTALACION DE CIELO RASO 12 M2**				
3.1	BALDOSA OWA TALCA MICROPERF "N" 2X4 14 MM (SAND)	PZA	22	S/. 10.50	S/. 231.00
3.2	PHOENIX GRID PRINCIPAL 3.66 M 10.08 KG/M2 15/16	PZA	6	S/. 10.25	S/. 61.50
3.3	PHOENIX GRID SECUNDARIO 1.22 M 10.08 KG/M2 15/16	PZA	18	S/. 2.75	S/. 49.50
3.4	PHOENIX GRID TERCIARIO 0.61 ML	PZA	18	S/. 2.50	S/. 45.00
3.5	PHOENIX GRID ANGULO 3.05 M 10.08 KG/M2 15/16	PZA	6	S/. 4.95	S/. 29.70
3.6	CLAVO DE CEMENTO 3/4 (ANG PERIMETRAL)	CTO	0.5	S/. 33.00	S/. 16.50
3.7	ALAMBRE GAL. # 16	KG	1	S/. 6.30	S/. 6.30
3.8	FULMINANTE PHOENIX CAL. 22 VERDE	CTO	1	S/. 11.00	S/. 11.00
3.9	CLAVO PHOENIX PIN CLIP 1 1/4" (32MM)	CTO	1	S/. 15.00	S/. 15.00
3.10	SERVICIO DE INSTALACION DE CIELO RASO SUSPENDIDO DE BALDOSA	M2	12	S/. 30.00	S/. 360.00
4.0	**SUMINISTRO E INSTALACION DE PISO TECNICO:** A) Altura de Base: 25cm B) Excelente resistencia a cargas fijas y dinamicas C) Reticulado metalico: Parte de baldosa estara embutida en un reticulado metalico D) La resistencia de cargas esta debidamente comprobada por el proveedor mediante. Contancias :ISO 9001 - SGS	M2	12.35	S/. 450.00	S/. 5,557.50
5.0	**SUMINISTRO E INSTALACION DE POZO TIERRA**				
5.1	OBRA CIVIL PREVIO (INC. EXCAVACION Y DEMOLICION)	M3	2	S/. 180.00	S/. 360.00
5.2	INSTALACION DE SISTEMA DE PUESTA A TIERRA (INC. Resistividad menos a 5 ohmios, para sistema informático)	GLB	2	S/. 2,800.00	S/. 5,600.00
6.0	**ACONDICIONAMIENTO DE DATA CENTER:**				
6.1	SUMINISTRO E INSTALACION DE PUNTOS DE RED CAT6 (REF. 30 ML, CANALETAS Y ACOMETIDA)	UND	2	S/. 850.00	S/. 1,700.00
6.2	CABLEADO DE ACOMETIDA TRIFASICA A TABLERO GENERAL (INC. ACOMETIDA, TUBERIA CONDUIT RIGIDA Y ACC. DE SUJECCION)	ML	80	S/. 50.00	S/. 4,000.00
6.3	TRASLADO E INSTALACION DE RACK DE BATERIAS Y UPS (REF. ALTURA DE 2 MTS)	GLB	1	S/. 2,500.00	S/. 2,500.00
6.4	SUMINISTRO E INSTALACION DE LUMINARIAS 60X60CM (INC. EQUIPO FLUORESCENTE, ACOMETIDA E INTERRUPTOR)	UND	4	S/. 280.00	S/. 1,120.00
6.5	DESMONTAJE E INSTALACION DE EQUIPO DE AIRE ACONDICIONADO 24 KBTU MARCA YORK (INC. EQUIPO, ACCESORIO DE INSTALACION Y ACOMETIDA)	UND	1	S/. 2,400.00	S/. 2,400.00
6.6	SUMINISTRO E INSTALACION DE PUERTA CONTRAINCENDIO CON CHAPA ANTIPANICO C/ SISTEMA DE ACCESO BIOMETRICO	UND	1	S/. 3,900.00	S/. 3,900.00
6.7	SUMINISTRO E INSTALACION DE GABINETE RACK HP 42RU	UND	2	S/. 2,650.00	S/. 5,300.00
	SISTEMA DE CANALIZACION CON CANASTILLAS Y ESCALERILLAS PARA				

6.8	LOS CABLES DE RED (INC. CANAL EN LA PARTE INFERIOR DEBAJO DEL PISO TECNICO Y PARTE SUPERIOR ENCIMA DEL FALSO CIELO)	GLB	1	S/. 2,100.00	S/. 2,100.00
6.9	SUMINISTRO E INSTALACION DE CAMARA DE SEGURIDAD IP	UND	1	S/. 1,200.00	S/. 1,200.00
6.10	DESMONTAJE E INSTALACION E SENSOR DE HUMO	UND	1	S/. 250.00	S/. 250.00
6.12	SERVICIO DE TRASLADO E INSTALACION EQUIPOS DE COMUNICACIÓN Y SISTEMA ELECTRICO AL NUEVO DATACENTER (MANO DE OBRA ESPECIALIZADA)	GLB	1	S/. 5,200.00	S/. 5,200.00
7.0	**OTROS GASTOS:**				
7.10	ACARREO DE DESMONTE Y LIMPIEZA DEL LOCAL	GLB	1	S/. 1,200.00	S/. 900.00
7.20	TRANSPORTE DE MATERIALES Y HERRAMIENTAS (ESCALERA, MATERIALES DE CONSTRUCCION)	GLB	1	S/. 1,800.00	S/. 1,800.00
				SUBTOTAL	S/. 48,837.00
				IGV 18% S/	S/. 8,790.66
				TOTAL S/	S/. 57,627.66

COSTO IMPLEMENTACIÓN DE DATA CENTER GOBIERNO REGIONAL PIURA
REFERENCIA: SUMINISTRO E INSTALACIÓN DE EQUIPOS DE PRECISIÓN
PROVEEDOR: COSUR SOLUCIONES INTEGRALES SAC

ITEM	DESCRIPCION	UNID	CANTIDAD	COSTO UNITARIO S./	COSTO TOTAL S./
1.0	**SUMINISTRO DE A.A PRECISION:** MARCA: SCHNEIDER MODELO : UNIFLAIR LE TDAR0511C + CAP0601PE CAP- TOTAL : 20.4 KW nominal a 23.9°C y 50% HR, con 46°C T. Condensador C. ELECTRICAS : 208/230V-3-60 REFRIGERANTE : ECOLOGICO R410 A COMPRESOR : SCROLL MICROPROCES.: MP-40 TARJETA RELOJ : CLOCK CARD HUMIDIFICADOR: 5 kg/h POR ELECTRODOS SUMERGIDOS RESISTENCIAS : 6KW FILTROS : EU-4 VENTILADORES : PALAS CURVADAS HACIA ATRÁS CONDENSADOR : CON REGULADOR DE PRESOSTATICO DE VELOCIDAD MONITOREO : TARJETA PCOWEB, TCP/IP ALARMAS : CONFIGURABLES CONTACTOS : CONTACTOS SECOS SENSORES : DETECTOR DE ANIEGOS	UND	1	S/. 78,750.00	S/. 78,750.00
2.0	**INSTALACION DE EQUIPO DE PRECISION:** Tablero de Distribucion Izaje y Monatje de Unid Condensadora y Evaporadora Tuberia de Cobre (Max 15m), Vacio, carga, pruebas Conexión a Punto electrico a 1m del equipo Conexión a Punto de Drenaje a 1m del equipo Conexión a Punto de Agua a 1m del equipo	UND	1	S/. 18,000.00	S/. 18,000.00

	Conexión a Punto de red a 1m del equipo Configuracion del microprocesador y monitoreo				
3.0	**SUMINISTRO E INSTALACION DE TABLERO A.A:** Suministro e instalacion de un Tablero Electrico de AA según recomendaciones del fabricante	UND	1	S/. 1,400.00	S/. 1,400.00
4.0	**OTROS GASTOS:**				
4.1	ACARREO DE DESMONTE Y LIMPIEZA DEL LOCAL	GLB	1	S/. 600.00	S/. 600.00
4.2	TRANSPORTE DE MATERIALES Y HERRAMIENTAS (ESCALERA, MATERIALES DE CONSTRUCCION)	GLB	1	S/. 700.00	S/. 700.00
			SUBTOTAL		S/. 99,450.00
			IGV 18% S/		S/. 17,901.00
			TOTAL S/		S/. 117,351.00

Anexo 13: Constancia de realización de tesis

CONSTANCIA

En mi calidad de Jefe de la Oficina de Tecnologías de Información del Gobierno Regional Piura, hago constar que **Javier Eduardo Delgado Mena**, estudiante de Ingeniería de Sistemas de la Universidad César Vallejo – Piura, identificado con **DNI 73823321**, realizó una investigación en la Institución que represento, como parte de la elaboración de su Tesis.

Se brindaron las facilidades para que la investigación continúe su curso de la mejor manera, proporcionando la información necesaria y colaborando en lo que fue solicitado.

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

Atentamente,

GOBIERNO REGIONAL PIURA
Oficina de Tecnologías de la Información - GGR

Ing. Víctor Manuel Mena Gutiérrez
Jefe de la Oficina de Tecnologías de Información